

# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ  
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION  
DEPARTMENT OF TELECOMMUNICATIONS

ANALÝZA VYSOKORYCHLOSTNÍCH SÍTÍ ZÁTĚŽOVÝM TESTEREM

BAKALÁŘSKÁ PRÁCE  
BACHELOR'S THESIS

AUTOR PRÁCE  
AUTHOR

OLEKSANDR YARMOLSKYY

BRNO 2015



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ  
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH  
TECHNOLOGIÍ  
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION  
DEPARTMENT OF TELECOMMUNICATIONS

## ANALÝZA VYSOKORYCHLOSTNÍCH SÍTÍ ZÁTĚŽOVÝM TESTEREM

HIGH-SPEED NETWORKS ANALYSIS USING LOAD TESTER

BAKALÁŘSKÁ PRÁCE  
BACHELOR'S THESIS

AUTOR PRÁCE  
AUTHOR

OLEKSANDR YARMOLSKYY

VEDOUCÍ PRÁCE  
SUPERVISOR

doc. Ing. VLADISLAV ŠKORPIL, CSc.

BRNO 2015



VYSOKÉ UČENÍ  
TECHNICKÉ V BRNĚ

Fakulta elektrotechniky  
a komunikačních technologií

Ústav telekomunikací

# Bakalářská práce

bakalářský studijní obor  
Teleinformatika

**Student:** Oleksandr Yarmolskyy

**ID:** 155262

**Ročník:** 3

**Akademický rok:** 2014/2015

## NÁZEV TÉMATU:

**Analýza vysokorychlostních sítí zátěžovým testerem**

## POKYNY PRO VYPRACOVÁNÍ:

Detailně prostudujte problematiku možností testování sítí a generování provozu. Seznamte se s jednotlivými referenčními měřeními prováděných v IP sítích. Seznamte se s technologií a zařízením IXIA, které je umístěno v laboratoři UTKO. Zaměřte se zejména na TCL API, IxExplorex, IxAutomate, ScriptGen a stručně popište ovládací, konfigurační a vývojové prostředí. Ve druhé části práce vytvořte tři vlastní laboratorní úlohy zaměřené na testování vybraných parametrů, uvažujte také využití TCL skriptů a IxAutomate. Užijte zapojení technologie CISCO v laboratoři, která by představovala zařízení pod zátěžovým testem, DUT (Device Under Test).

## DOPORUČENÁ LITERATURA:

[1] PUŽMANOVÁ, R. Moderní komunikační sítě A-Z. Computer Press, Brno 2007

[2] IXIA, firemní dokumentace, stránky <http://www.utko.feec.vutbr.cz/~skorpil/fpga>

**Termín zadání:** 9.2.2015

**Termín odevzdání:** 2.6.2015

**Vedoucí práce:** doc. Ing. Vladislav Škorpil, CSc.

**Konzultanti bakalářské práce:**

**doc. Ing. Jiří Mišurec, CSc.**

*Předseda oborové rady*

## UPOZORNĚNÍ:

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

## **ABSTRAKT**

Tato bakalářská práce se zabývá návrhem laboratorních úloh pro předmět zabývající se vysokorychlostními sítěmi. Teoretická část popisuje gigabitový Ethernet, typické prvky v sítích, jako jsou přepínače a směrovače, testy z RFC 2544 a programové nástroje IXIA na provádění testování, mezi něž patří IxAutomate, IxExplorer. V praktické části jsou vytvořeny návrhy laboratorních úloh, zaměřených na testování různých možností nastavení přepínačů, směrovačů a vlastností linkové a síťové vrstvy. Součástí práce jsou prezentace k úlohám a koncové konfigurace nastavení IXIA programů v podobě TCL skriptů pro jednotlivé úlohy.

## **KLÍČOVÁ SLOVA**

IXIA, IxExplorer, IxAutomate, přepínač, směrovač, síť, QoS, Cisco

## **ABSTRACT**

This thesis describes the design of laboratory tasks for a subject dealing with high-speed networks. The theoretical part describes Gigabit Ethernet, the typical elements in the network, such as switches and routers, RFC 2544 tests and software tools for the implementation of IXIA testing, including IxAutomate, IxExplorer. In the practical part designs are created laboratory exercises aimed at testing different options switches, routers and properties of line and network layers. The work tasks and presentations to end configuration settings IXIA programs in the form TCL scripts for each job.

## **KEYWORDS**

IXIA, IxExplorer, IxAutomate, Switch, Router, Network, QoS, Cisco

YARMOLSKYY, Oleksandr *Analýza vysokorychlostních sítí zátěžovým testerem*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2015. 67 s. Vedoucí práce byl doc. Ing. Vladislav Škorpil, CSc.

## PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Analýza vysokorychlostních sítí zátěžovým testerem“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno .....

.....

(podpis autora)

## PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu bakalářské práce panu doc. Ing. Vladislavu Škorpilovi, CSc. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci. Také děkuji Ing. Václavu Oujezskovi za cenné rady při práci.

Brno .....

.....

(podpis autora)

## PODĚKOVÁNÍ

Výzkum popsáný v této bakalářské práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

Brno .....

.....  
(podpis autora)

# OBSAH

<b>Úvod</b>	<b>12</b>
<b>1 Technologie Ethernet</b>	<b>13</b>
1.1 Gigabit Ethernet . . . . .	14
1.1.1 Linková vrstvá . . . . .	14
1.1.2 Fyzická vrstvá . . . . .	15
1.1.3 Standardy Gigabit Ethernetu . . . . .	16
<b>2 Popis typických prvků v sítích</b>	<b>17</b>
2.1 Přepínač . . . . .	17
2.1.1 Vnitřní struktura přepínače obecně . . . . .	19
2.2 Směrovač . . . . .	20
<b>3 Možnosti testování sítí</b>	<b>21</b>
3.1 RFC 2544 . . . . .	21
3.1.1 Propustnost (Throughput) . . . . .	21
3.1.2 Zpoždění (Latency) . . . . .	22
3.1.3 Ztrátovost (Frame/Packet loss rate) . . . . .	22
3.1.4 Back-to-back . . . . .	22
3.1.5 Zotavení po přetížení (System recovery) . . . . .	23
3.1.6 Zotavení po restartu (System reset) . . . . .	23
<b>4 Popis nástrojů na analýzu sítí</b>	<b>24</b>
4.1 Generátor provozu IXIA . . . . .	24
4.2 IxExplorer . . . . .	25
4.2.1 Stručný popis IxExploreru . . . . .	25
4.3 IxAutomate . . . . .	27
4.3.1 Stručný popis IxAutomate . . . . .	27
4.4 ScriptGen . . . . .	28
<b>5 Návrh laboratorních úloh</b>	<b>31</b>
5.1 Laboratorní úloha 1 . . . . .	31
5.1.1 Topologie měření . . . . .	31
5.1.2 Potřebná výbava . . . . .	31
5.1.3 Úvod . . . . .	32
5.1.4 Příprava přepínače . . . . .	34
5.1.5 Nastavení IxAutomate a zahájení testu . . . . .	37
5.2 Laboratorní úloha 2 . . . . .	41



5.2.1	Topologie měření . . . . .	42
5.2.2	Potřebná výbava . . . . .	42
5.2.3	Úvod . . . . .	42
5.2.4	Příprava přepínače . . . . .	44
5.2.5	Nastavení IxExplorer a zahájení testu . . . . .	48
5.3	Laboratorní úloha 3 . . . . .	52
5.3.1	Topologie měření . . . . .	52
5.3.2	Potřebná výbava . . . . .	52
5.3.3	Úvod . . . . .	53
5.3.4	Příprava směrovačů . . . . .	54
5.3.5	Nastavení IxExplorer a zahájení testu . . . . .	56
<b>6</b>	<b>Závěr</b>	<b>61</b>
	<b>Literatura</b>	<b>62</b>
	<b>Seznam symbolů, veličin a zkratk</b>	<b>64</b>
	<b>Seznam příloh</b>	<b>66</b>
<b>A</b>	<b>Obsah přiloženého CD</b>	<b>67</b>

# SEZNAM OBRÁZKŮ

1.1	Popis vrstev ISO/OSI a TCP/IP modelu . . . . .	13
1.2	Zařazení Gigabit Ethernetu do referenčního modelu . . . . .	14
1.3	Popis vrstev GbE . . . . .	15
2.1	Hierarchické uspořádání přepínačů v sítích . . . . .	18
2.2	Blokové uspořádání uvnitř přepínače . . . . .	19
4.1	Generátor provozu IXIA . . . . .	24
4.2	Zadání adresy šasi . . . . .	25
4.3	Okno programu IxExplorer po připojení k šasi . . . . .	26
4.4	Nastavení skupin toku dat . . . . .	26
4.5	Zobrazení statistik na portu 3 . . . . .	27
4.6	Okno programu po spuštění . . . . .	28
4.7	Průběh testu Frame Error Filtering . . . . .	29
4.8	Grafické zobrazení statistiky měření . . . . .	29
4.9	Vytvoření TCL skriptu pomocí ScripGen programu . . . . .	30
5.1	Zapojení úlohy v laboratoři . . . . .	31
5.2	Výsledný výstup příkazu show ip interface brief . . . . .	34
5.3	Výsledný výstup příkazu show policy-map pro ověření konfigurace politik . . . . .	36
5.4	Výsledný výstup příkazu show policy-map interface g0/14 pro ověření aplikace politiky na rozhraní . . . . .	36
5.5	Část výstupu příkazu show run . . . . .	37
5.6	Nastavení chasis . . . . .	38
5.7	Nastavení parametrů testu . . . . .	38
5.8	Nastavení směru provozu . . . . .	39
5.9	Zaznamenávání průběhu testu v záložce <i>Logs</i> . . . . .	40
5.10	Ukázka grafického zobrazení výsledku testu . . . . .	40
5.11	Výsledné grafické zobrazení výsledků v opačném směru provozu . . . . .	41
5.12	Zapojení úlohy v laboratoři . . . . .	42
5.13	Umístění CoS bitů v hlavičce rámce . . . . .	43
5.14	Výstup příkazu show mls qos maps cos-input-q . . . . .	47
5.15	Výstup příkazu show mls qos maps cos-output-q . . . . .	47
5.16	Výstup příkazu show mls qos input-queue . . . . .	47
5.17	Výstup příkazu show mls qos queue-set (v úloze nastaven set 2) . . . . .	48
5.18	Tlačítko Add/Remove field from the table . . . . .	48
5.19	Ukázka aktivování MAC adresy Ixia na portu 02 se změnou posledního znaku . . . . .	49
5.20	Nastavení streamů . . . . .	49

5.21	Nastavení MAC adres . . . . .	49
5.22	Označená tlačítka na start/stop zachytávání a start/stop streamů . .	50
5.23	Výsledné zpoždění a bitový tok . . . . .	51
5.24	Zapojení úlohy v laboratoři . . . . .	52
5.25	Výstup příkazu traceroute na CE směrovač . . . . .	54
5.26	Výstup příkazu show ip int br na PE1 . . . . .	54
5.27	Výstup příkazu show ip route na PE1 . . . . .	55
5.28	Výstup příkazu show ip interface brief na P1 . . . . .	55
5.29	Výstup příkazu show ip route PE2 . . . . .	56
5.30	Nastavení protocol managementu . . . . .	56
5.31	Nastavení IP adres IXIA portu a směrování mezi nimi . . . . .	57
5.32	Nastavení MAC adres . . . . .	57
5.33	Nastavení ARP protokolu . . . . .	57
5.34	Nastavení packet streamu . . . . .	57
5.35	Ukázka zobrazení statistik obou portů vedle sebe . . . . .	58
5.36	Ikona pro nastavení časování . . . . .	58
5.37	Nastavení doby přenosu . . . . .	58
5.38	Ikona na start streamu . . . . .	59
5.39	Ikona na zastavení streamu . . . . .	59
5.40	Předpokládané výsledky ztrátovosti paketů . . . . .	59

# SEZNAM TABULEK

1.1	Přehled některých standardů GbE . . . . .	16
3.1	Propustnost různých velikostí rámců při 1000 Mbit/s . . . . .	22
5.1	Doporučená klasifikace provozů podle IEEE . . . . .	44

# ÚVOD

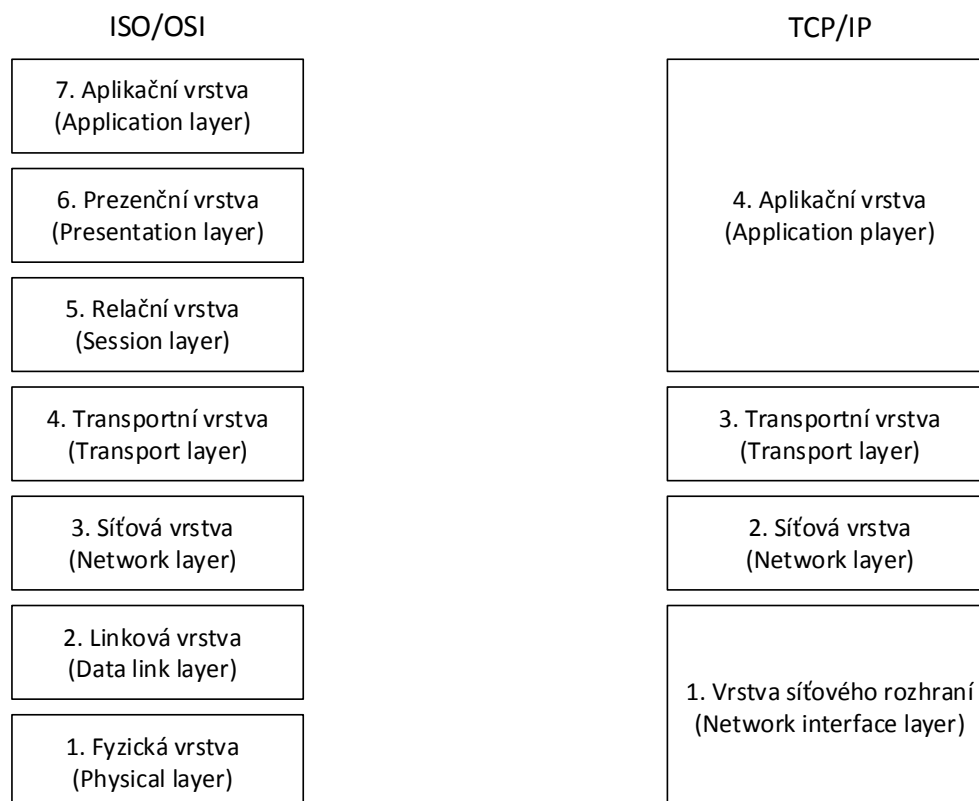
Práce se zabývá problematikou testování vysokorychlostních sítí. Konkrétně vlastnosti linkové a síťové vrstvy při různých možnostech nastavení Cisco přepínače a směrovače. Práce se skládá ze dvou pomyslných částí. První je teoretická, kde je úvod do problematiky v podobě stručného popisu Ethernetu, gigabitového Ethernetu, typických prvků v sítích, což nejčastěji jsou přepínače a směrovače, testu z RFC 2544, které byly nejvíce využité v práci a nakonec stručný popis nástrojů IXIA zařízení, mezi něž patří programy IxAutomate, IxExplorer a ScripGen.

V praktické části jsou navrženy úlohy v prostředí IXIA zařízení a Cisco IOS operačního programu. Dvě úlohy se zabývají problematikou linkové vrstvy s čímž souvisí přepínání rámců a nastavení přepínače, jako např. politiky, omezování provozu, QoS apod. Třetí úloha se už věnuje síťové vrstvě, kde je měřená rychlost konvergence OSPF protokolu. Úlohy jsou koncipované tak, aby studenta uvedli stručně do problematiky a naučily nějaké nové konfigurace navíc, které by se mohly hodit v praxi nebo dalším studiu. K úlohám je i návod „krok za krokem“ pro nastavování zařízení, nástrojů IXIA a popis správného vyhodnocování výsledků.

Pro doplnění tu jsou vypracované prezentace ke každé úloze a pro případ kdyby studenti nakonfigurovali něco špatně, jsou dostupné koncové konfigurace obslužných programů zařízení IXIA. Prezentace i koncové konfigurace jsou v příloze.

# 1 TECHNOLOGIE ETHERNET

Technologie Ethernet je název pro souhrn technologií používaných v lokálních počítačových sítích (LAN) - vychází z názvu éter - imaginární všudypřítomné látky v okolním prostoru. Nyní se jedná o nejperspektivnější a nejrozšířenější technologii (poměr cena/výkon, jednoduchý návrh, snadné přizpůsobení pro nové technologie v budoucnu...). Existují různé typy podle rychlosti a použitého média.



Obr. 1.1: Popis vrstev ISO/OSI a TCP/IP modelu

Ethernet je definován na fyzické a linkové vrstvě referenčního modelu ISO/OSI 1.1 a na vrstvě síťového rozhraní modelu TCP/IP 1.1. Spadá do standardů IEEE (Institute of Electrical and Electronics Engineers) 802.3. Byl vyvinut firmou DEX, Intel a Xerox (DIX-Ethernet) v letech 1972-1975. Experimentální síť tehdy pracovala s rychlostí 2,94 Mbit/s.

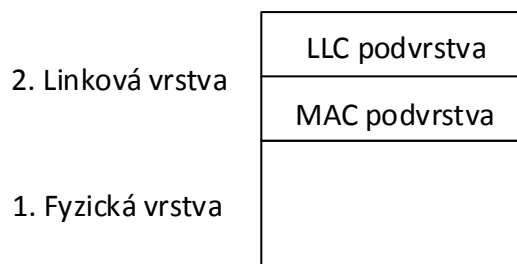
Pro přístup k mediu využívá metodu CSMA/CD. První komerční verze byla představená v roce 1980 s přenosovou rychlostí 10 Mbit/s (10BASE5). DIX-Ethernet byl později mírně upraven na Ethernet II pro lepší kompatibilitu se standardem IEEE. Větší rozdíl byl jen ve formátu rámce. Ethernet, již po roce 1990 se stal

nejpoužívanější technologii a vytlačil ostatní způsoby propojení mezi počítači. Nyní mu jsou konkurenci pouze bezdrátové sítě.

V červnu 1998 byl schválen gigabit Ethernet a v březnu 1999 vznikla pracovní skupina Higher Speed Study Group (HSSG). Jejím úkolem bylo vyvíjet desetigigabitový ethernet. Práce byla dokončena v červnu 2002 a standard dostal označení IEEE 802.3ae. Při takto velkých rychlostech už se využívá jen plně duplexní provoz a většinou jako médium slouží optická vlákna. Takže odpadá přístupová metoda CSMA/CD [4] [10] [17].

## 1.1 Gigabit Ethernet

První standard IEEE 802.3z vyšel v roce 1998 pod označením 1000BASE-X. Ratifikovaný byl v roce 1999 pod standardem IEEE802.3ab a označením 1000BASE-T. Gigabit Ethernet (GbE nebo 1 GigE, dále jen GbE) je nejčastěji vedený přes UTP kabel cat (Category) 5, 5e nebo 6. Linková vrstva obsahuje dvě podvrstvy - LLC a MAC, viz dále. Souvislost s referenčním modelem je na obrázku 1.2 [10].



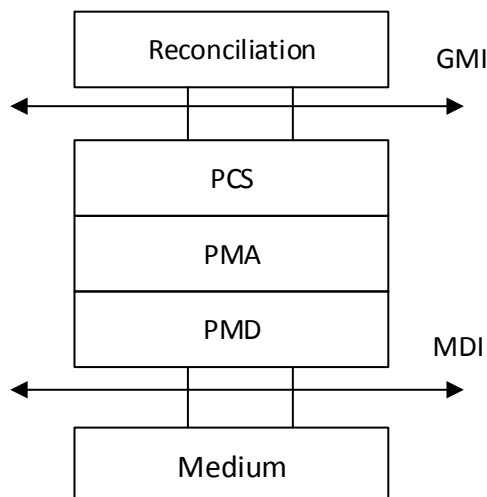
Obr. 1.2: Zařazení Gigabit Ethernetu do referenčního modelu

### 1.1.1 Linková vrstva

Jako ostatní verze má i GbE dvě podvrstvy - LLC (Logical Link Control) a MAC (Media Access Control). Podvrstva LLC zodpovídá za řízení logického spoje. Formát hlavičky LLC nezávisí na typu sítě. Podvrstva MAC slouží k řízení přístupu na přenosové médium. Také provádí detekci chyb pomocí CRC součtu [10].

### 1.1.2 Fyzická vrstvá

Vychází z fyzické vrstvy sítě Fibre Channel. Oproti ostatním verzím se fyzická vrstva GbE liší tím, že má tři hlavní podvrstvy. **Reconciliation** je vyrovnávací podvrstva. **GMII** a **MDI** jsou rozhraní, viz obrázek 1.3 [10]:



Obr. 1.3: Popis vrstev GbE

**PCS** - Physical Coding Sublayer - kódování a dekódování (8b/10b), řeší proces automatického nastavení komunikační rychlosti a zajišťuje synchronizaci.

**PMA** - Physical Medium Attachment - provádí převod mezi paralelním a sériovým tokem dat a obnovuje signál při příjmu. Bufferováním celé desetibitové kódové skupiny při příjmu zavádí zpoždění odpovídající době přenosu 10 bitů.

**PMD** - Physical Medium Dependent - popisuje konkrétní vlastnosti vysílače a přijímače signálu (výkonové úrovně signálů).

**GMII** - Gigabit Medium Independent Interface - zajišťuje paralelní přenos 8 bitů s taktovacím kmitočtem 125 Mbaud. Kromě toho obsahuje další řídicí signály - časovací signál, detekce nosné, chyba přenosu, apod. Nespecifikuje však typ konektoru pro připojení gigabitového transceiveru kabelem, jak to bylo u rozhraní AUI pro desetimegabitový Ethernet a MII pro stomegabitový Ethernet.

**MDI** - Medium Dependent Interface - definuje konektory, pro 1000 BASE-SX a 1000BASE-LX jsou definovány duplexní konektory typu SC.



### 1.1.3 Standardy Gigabit Ethernetu

Na GbE existuje spousta standardů, jak na optiku (single mode i multimode), tak na metaliku. Existují i standardy na měděný vyrovnaný kabel s označením CX u konce (1000BASE-CX). V tabulce 1.1.3 je výčet nejrozšířenějších standardů pro GbE [10].

Tab. 1.1: Přehled některých standardů GbE

Standard	Médium	Max. vzdálenost
1000BASE-CX	Twinaxiální kabel	25 m
1000BASE-SX	MM	220-550 m
1000BASE-LX	MM	550 m
1000BASE-LX	SM	5 km
1000BASE-LX10	SM	10 km
1000BASE-ZX10	SM	70 km
1000BASE-BX10	SM, 1490/1310 nm down/up	10 km
1000BASE-T	Kroucená dvojlinká (cat5, 6e, 6, 7)	100 m
1000BASE-TX	Kroucená dvojlinká (cat6 a 7)	100 m

## 2 POPIS TYPICKÝCH PRVKŮ V SÍTÍCH

Prvky v sítích ethernetu jsou huby, repeatery (opakovače), mosty (bridge), přepínače (switche) a směrovače (routery). Huby už se nepoužívají, jen v ojedinělých případech a repeatery u velkých vzdáleností (optika). Jelikož přepínače a směrovače jsou typické a nejpoužívanější prvky v dnešních sítích LAN, které můžeme potkat (ať už softwarově nebo hardwarově), je má práce věnovaná návrhu laboratorních úloh právě s těmito prvky. Proto je nutné pro lepší pochopení a obrázek problematiky, stručně popsat tyto dva síťové prvky.

### 2.1 Přepínač

Přepínač je aktivní síťový prvek, který se stará o zasílání rámců a dělí síť Ethernet na kolizní domény. Nahradil dříve používané rozbočovače (huby). Pracuje na linkové vrstvě 1.1 referenčního modelu ISO/OSI, ale existují i kombinované přepínače, co pracují na linkové, síťové a vyšších vrstvách. Na přepínání mu slouží tabulka CAM (Content Addressable Memory) v níž jsou obsaženy MAC adresy - fyzické (Media Access Control) adresy. Adresy do této tabulky se dají získat dvojím způsobem. První je automatické učení z provozů sítě, kdy si přepínač zapamatuje, odkud rámec přišel. V průběhu učení posílá příchozí rámce na všechny porty, protože ještě neví konkrétní cílovou adresu (posílá broadcasty). Druhá možnost je manuální přidání určité adresy do tabulky. Používá se pro zvýšení bezpečnosti v síti.

Jak již bylo uvedeno výše, rozděluje síť na kolizní domény. Na každém portu se nachází jedna doména a každý port dokáže pracovat v plně duplexním režimu s různou rychlostí přenosu (10, 100, 1000 Mbit/s). Pro rychlejší přenosy (10, 40 Gbit/s) jsou dražší přepínače, ale ty se používají pouze pro tzv. páteřní a distribuční vrstvy sítě, viz. 2.1. Na těchto dvou vrstvách se vyžadují obzvláště rychlé a pokročilé přepínače (hlavně páteřní) pro co nejrychlejší přenos dat. Na přístupové vrstvě pro rozdělení všesměrových domén se vytvářejí VLAN (Virtual LAN), které umožňují efektivně využívat systémové prostředky.

Dále se rozděluje podle způsobu a rychlosti práce s rámcem. Podle toho jaká je použitá technologie a funkce v přepínači se odvíjí její cena. Je třeba si všimnout, že menší rámce rychleji projdou přes přepínač a rychleji zvýší zátěž sítě, proto je někdy výhodnější zvýšit velikost rámce. V současnosti existují tyto způsoby přeposílání rámců [9]:

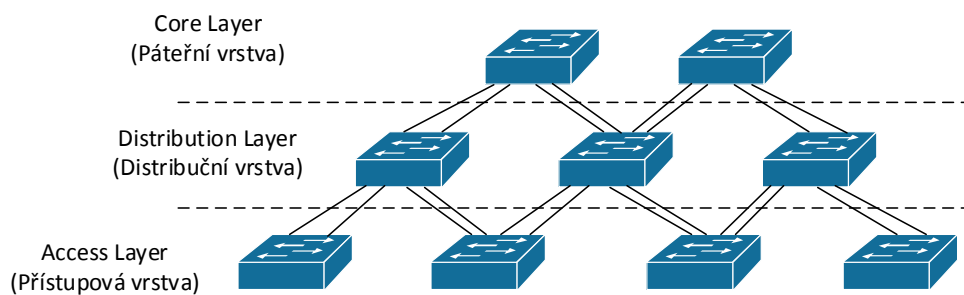
**Store and forward** - Přijatý rámec je uložen do vyrovnávací paměti (bufferu).

Následně se prohlédne jeho hlavička, zkontroluje FCS (Frame Check Sequence) a nakonec je poslán na určité rozhraní.

**Cut-through** - Používá se pro nejrychlejší přeposílání rámců. Načte se pouze začátek rámce pro zjištění MAC adresy cíle. Přepínače s touto metodou mívají minimální zpoždění.

**Fragment free** - Používá se při připojení hubu na port. Rámec je přeposlán až po 64 B, kdy už nehrozí, že by na segmentu mohla být kolize.

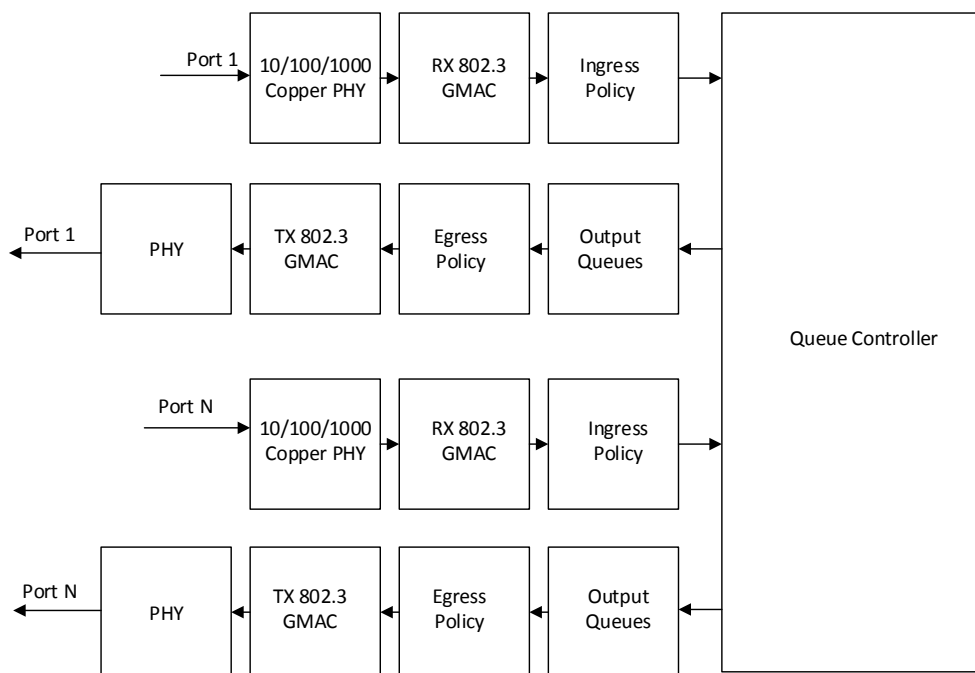
**Adaptive switching** - Přepínání mezi metodami Store and forward a Cut-through podle aktuálního zatížení sítě.



Obr. 2.1: Hierarchické uspořádání přepínačů v sítích

### 2.1.1 Vnitřní struktura přepínače obecně

Pro lepší pochopení problematiky testování přepínačů na linkové vrstvě, je dobré si prohlédnout vnitřní blokovou strukturu přepínače. Na 2.2 je příklad multiportového, gigabitového přepínače s popisem hlavních bloků účinkujících v zpracování rámců [13].



Obr. 2.2: Blokové uspořádání uvnitř přepínače

**PHY** - Fyzické rozhraní, které přijímá a vysílá rámce z/do Gigabit MAC (GMAC).

**GMAC** - Gigabit Media Access Controller je zodpovědný za formátování rámce, stripping, FCS, CSMA/CD a vypořádání se s kolizemi.

**Ingress Policy** - Kontroluje přicházející rámce, jestli mají QoS prioritu pro Queue controllera (kontrolér front). Implementuje a vybírá funkce jako Port Based VLANs nebo 802.1Q VLANs (tagování).

**Queue Controller** - Hlavní část přepínače, která řídí přepínání rámců.

**Output Queues** - Vysílá rámce podle pořadí ve frontě s určitou prioritou. Rychlost s jakou se zpracují, se mění v závislosti na rychlosti portu a zahlcení sítě.

**Egress Policy** - Kontroluje vycházející rámce a modifikuje je podle potřeby (Port based VLANs, Tagging/Un-tagging od 802.1Q).

## 2.2 Směrovač

Směrovač je aktivní síťový prvek pracující na síťové vrstvě ISO/OSI 1.1. Jeho nejdůležitější funkcí je směrování paketů v sítích podle směrovací tabulky. Tuto funkci mu umožňují směrovací protokoly (RIPv1-2, OSPF, EIGRP, BGP) na základě kterých směrovač volí nejlepší cestu. Rozděluje síť na všesměrové (broadcastové) domény. Kvůli výměně informací mezi protokoly, by měl vždy pracovat v plně duplexním režimu.

Směrovací tabulka se může sestavit dvěma způsoby. Statický, pro menší sítě, nevyžaduje velký výpočetní výkon hardwaru (HW) směrovače a velké znalosti obsluhy, nebo Dynamický. Dynamický se hodí pro větší síť nebo pro síť, kde nastávají často změny, vyžaduje větší výkon HW a větší znalosti obsluhy. V praxi se kombinuje obojí.

Dále směrovače mají méně portů než přepínače - více se ani nevyžaduje, protože zasílají informaci pouze na další směrovače (resp. síť), tj. pár linek na sousedy. Dělí se podle použití na různě pokročilé s různou funkcí, nastavením a výkonem. Rychlosti portů jsou většinou 10, 100, 1000 Mbit/s a pro směrovače na páteřních linkách 10, 40 Gbit/s, kde jsou potřeba nejvýkonnější směrovače s podporou velkých přenosových rychlostí. Dají se na nich nastavit různé politiky směrování paketů pomocí ACL (Access List) avšak čím více politik je, tím větší nároky na směrovač jsou (CPU využití) [9].

## 3 MOŽNOSTI TESTOVÁNÍ SÍTÍ

V této kapitole budou probírané možnosti testování sítí na linkové a síťové vrstvě. Zájmena se jedná o testy RFC 2544 pro testování přepínačů a směrovačů.

Testování v Ethernetu se provádí pro ověření správné činnosti zařízení při určitých úrovních provozů v sítí, např. zvýšený provoz. Specifikace těchto testů, jako procedury pro činnost, velikosti rámců, trvání testu a počet iterací, jsou popsány mezinárodní organizací IETF.

Mezinárodní organizace IETF (Internet Engineering Task Force) má několik pracovních skupin. Skupina, která se věnuje metodice testování sítí, se nazývá Benchmarking Methodology Working Group (BMWG). Má několik doporučení v dokumentech Request For Comments (RFC), které jsou k nahlédnutí komukoliv na internetu. Vylepšením a zavedením nových metodik se věnují i nadále, kdy každoročně pořádají několik konferenci na dané téma.

### 3.1 RFC 2544

Toto doporučení bylo vydáno prvně v roce 1999. Nahradilo tehdy už nepraktické RFC 1944, ale přebírá terminologii a některé pojmy z ještě staršího RFC 1242. Definuje měření propustnosti, zpoždění, ztrátovosti, back-to-back pakety/rámce, zotavení po přetížení a zotavení po restartu. Parametr kolísání (jitter) ještě není definován, ale v analyzátorech je přítomný [11] [14].

#### 3.1.1 Propustnost (Throughput)

Propustnost definuje maximální počet rámců (resp. paketů) za sekundu při kterém nenastane chyba (např. ztráta rámce, apod.). Používá se pro zjištění přenosových limitů přepínače (resp. směrovače - pakety). Výsledná propustnost je pro každou délku rámce odlišná, jak je uvedeno v tabulce 3.1.1. Důvodem je mezirámcová mezera, která je nejpatrnější u malých délek rámců - přenese se jich nejvíce a je nutná větší mezera mezi nimi.

Měření se provádí tak, že nejdříve se pošlou rámce na DUT (Device Under Test) s maximální přenosovou rychlostí. Dále se porovná počet odeslaných a přijatých rámců. Pokud nastane chyba nebo ztráta rámce, přenosová rychlost se sníží na polovinu a test se opakuje. Pokud chyba nebo ztráta rámce nenastane, přenosová rychlost se zvýší o polovinu rozdílu přenosové rychlosti posledního a předposledního měření [11] [14].

Tab. 3.1: Propustnost různých velikosti rámců při 1000 Mbit/s

Velikost rámce	Propustnost	Preamble a IGP	Rámců/s
64B	761,90 Mbit/s	238,10 Mbit/s	1 488 095
128B	864,86 Mbit/s	135,14 Mbit/s	844 594
256B	927,54 Mbit/s	72,46 Mbit/s	452 898
512B	962,40 Mbit/s	37,59 Mbit/s	234 962
1024B	980,84 Mbit/s	19,16 Mbit/s	119 731
1280B	984,61 Mbit/s	15,38 Mbit/s	96 153
1518B	986,99 Mbit/s	13,00 Mbit/s	81 274
1522B	987.02 Mbit/s	12,97 Mbit/s	81 063

### 3.1.2 Zpoždění (Latency)

Test zpoždění určuje čas cesty rámce (resp. paketu) od vysílacího zařízení k cílovému zařízení (DUT). Existují dva typy měření, jednosměrné a obousměrné. Jednosměrné je pouze cesta od zdroje k cíli. Obousměrné (Round-Trip Time) zpoždění je cesta od zdroje k cíli a zpět. Zpoždění je nežádoucí u služeb v reálném čase, hlavně u přenosu videa a zvuku.

Měří se při maximální propustnosti, při které nedochází k chybě (ztrátě), po dobu 120s. Pro každou délku rámce se měří zvlášť a to 20x. Výsledné zpoždění je průměrem těchto měření [11] [14].

### 3.1.3 Ztrátovost (Frame/Packet loss rate)

Ztrátovost určuje schopnost DUT vypořádat se s rámcí (nebo pakety) při velké zátěži sítě. Tuto vlastnost je třeba znát při použití služeb v reálném čase, protože velká ztrátovost způsobuje výpadky v obraze (kostky) a zvuku (pauzy, nesrozumitelnost). Rámce mohou být ztráceny z různých důvodů, např. chyba v součtu FCS, nadměrné zpoždění v zpracování apod.

Měří se při maximální propustnosti sítě, kdy se zjišťuje jestli při přenosu nastala chyba, tj. ztráta rámce. Pokud nastala, sníží se rychlost o nastavitelný krok (podle doporučení je maximum 10%) a znovu se provede měření pro novou rychlost. Měří se do doby, kdy po dvou měřeních za sebou je nulová ztrátovost [11] [14].

### 3.1.4 Back-to-back

Test Back-to-back, též známý jako burstability nebo burst test, prověřuje schopnosti bufferu u prepínače (resp. směrovače).

Back-to-back test probíhá tak, že se pošle shluk (burst) rámců s minimální mezirámcovou mezerou směrem k DUT. Následně se počítá počet rámců přeposlaných DUT. Když je počet zaslaných rámců k DUT roven počtu rámců přeposlaných z DUT, je burst zvýšen a test je znovu spuštěn. Když je nějaký rámec ztracen, je burst zmenšen. Zkušební doba shluku má mít minimálně 2s a opakovat se 50x [11] [14].

### **3.1.5 Zotavení po přetížení (System recovery)**

Tento test zjišťuje rychlost zotavení DUT z přetíženého stavu. Je proveden zasláním rámců s rychlostí 110%, zaznamenané z měření propustnosti, po dobu 60s. Časové razítko A sníží přenosovou rychlost rámců o 50% a zaznamená se čas, kdy se ztratil poslední rámec kvůli přetížení (časové razítko B). Výsledná doba zotavení se vypočítá jako rozdíl časových razítek, tj.  $A - B$  [11] [14].

### **3.1.6 Zotavení po restartu (System reset)**

Úkolem tohoto testu je zjistit rychlost s jakou se DUT zotavuje z restartu. Restart může být hardwarový (HW) nebo softwarový (SW).

Čas zotavení se určí odesláním rámců s nejmenší možnou délkou a maximální přenosovou rychlostí, zjištěnou z měření propustnosti. Při zasílání se provede restart DUT. Dále se zaznamená čas, kdy byl přijat poslední rámec před restartem a čas, kdy byl rámec přijat po restartu. Rozdíl těchto časů je čas zotavení po restartu [11] [14].



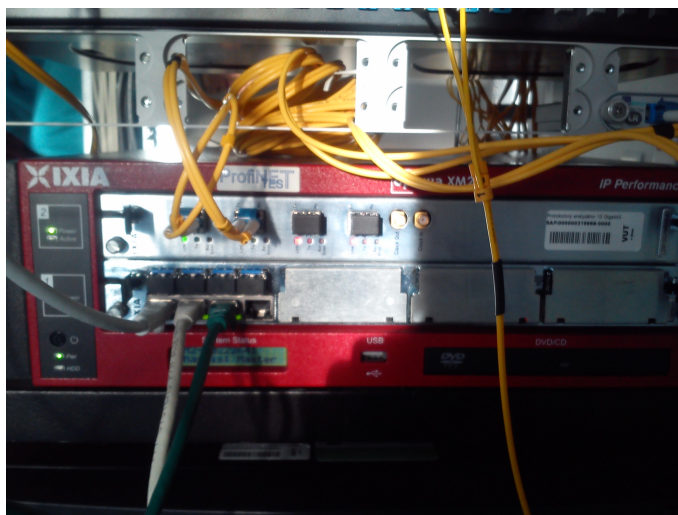
## 4 POPIS NÁSTROJŮ NA ANALÝZU SÍTÍ

V této kapitole budou popsány nástroje na analýzu sítí. Jedná se o analyzátor IXIA, který generuje a analyzuje síťový provoz a balíček programu k němu. Nástroje mají možnost konfigurace vlastních testů pomocí TCL skriptů. Lze podle potřeby upravit i testy z RFC 2544.

### 4.1 Generátor provozu IXIA

Analyzátor IXIA slouží k testování výkonnostních parametrů síťových prvků a sítí, jako 10, 100, 1000 Mbit/s Ethernet, 10 Gbit Ethernet, ATM a Packets over SONET. Z prvků se jedná zejména o přepínače, směrovače a firewally. Testuje na fyzické, linkové, síťové a transportní vrstvě ISO/OSI modelu. Generuje různé druhy provozu až po plně duplexní. Zvládá duplexní provoz s maximální rychlostí 10 Gbit/s na všech rozhraních najednou. Umí generovat a analyzovat rámce o různých délkách, tj. od 64 B až po 1512 B - pro určité testy méně i více. Na obrázku 4.1 je ukázka, jak generátor vypadá, při zapojení na DUT (přepínač Cisco).

Generátor běží na operačním systému Windows XP, ale neumožňuje vylepšení na vyšší verze. Dá se ovládat přímo s integrovanými obslužnými programy, ale doporučuje se spouštět obslužný software na jiném počítači a vzdáleně se přes tyto programy připojovat na generátor. Obslužné programy ke generátoru jsou IxAutomate a IxExplorer [6].



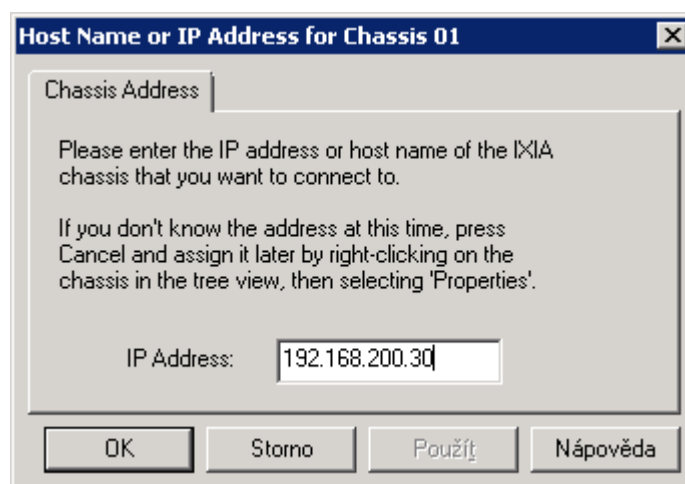
Obr. 4.1: Generátor provozu IXIA

## 4.2 IxExplorer

Program IxExplorer slouží na programování hardwaru Ixia generátoru a provádění testů v síti. Testuje na fyzické až transportní vrstvě. Každá vrstvá je nezávislá, tj. generátor pro ni zvlášť generuje a analyzuje provoz a neovlivňují se ostatní vrstvy. V případě nestavového protokolu, provádí správu až na aplikační vrstvě. Dokáže generovat maximálně 255 provozních toků. Vždy na jednom rozhraní generuje a na druhém provádí analýzu. Podle potřeby lze pro různé testy upravovat hlavičky rámců nebo paketů [7].

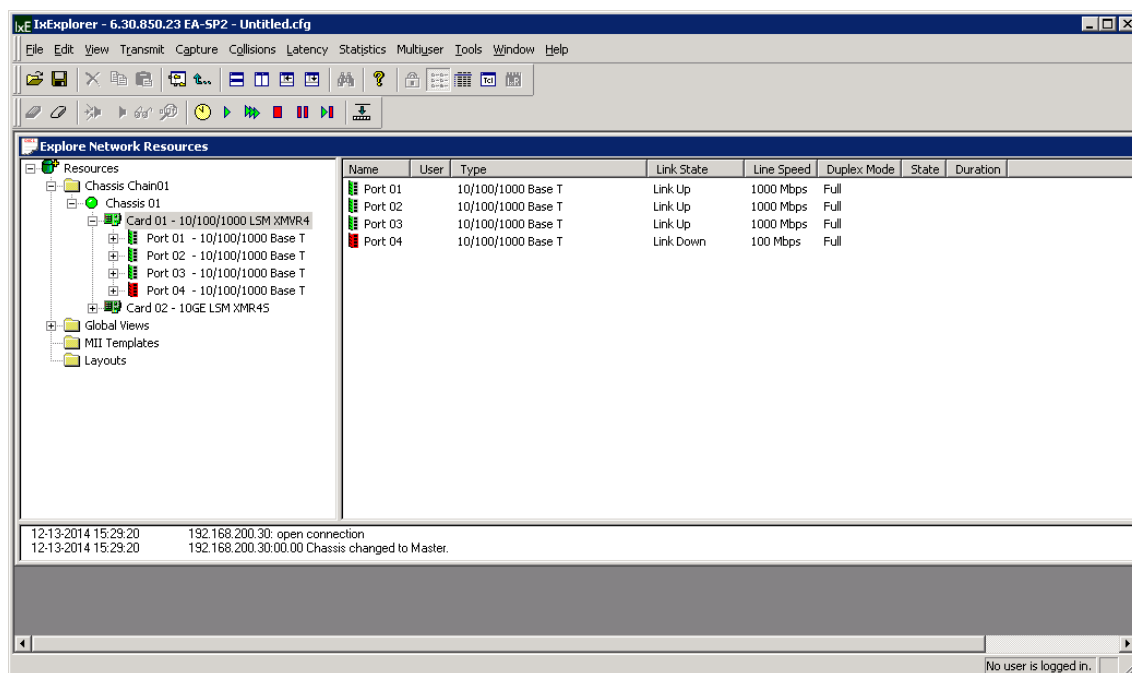
### 4.2.1 Stručný popis IxExploreru

Před samotným měřením je nutné se připojit k šasi, na které chceme provádět měření. Adresa šasi v laboratoři je 192.168.200.30, viz 4.2. Na obrázku 4.3 je ukázka okna programu po zadání adresy šasi.



Obr. 4.2: Zadání adresy šasi

V horní části obrázku 4.3 je klasické menu pro navigaci a nastavení v programu (jako File, Edit, View...). V levé části je menu „Network Resources“. Zde se nastavují a spravují po rozkliknutí *Chassis* (Šasi) - *Card* (Karta) - *Port* (Port). Po označení portu, se otevře okno (v programu vpravo), kde se nastavují provozní toky, velikosti rámců/paketů a další parametry.



Obr. 4.3: Okno programu IxExplorer po připojení k šasi

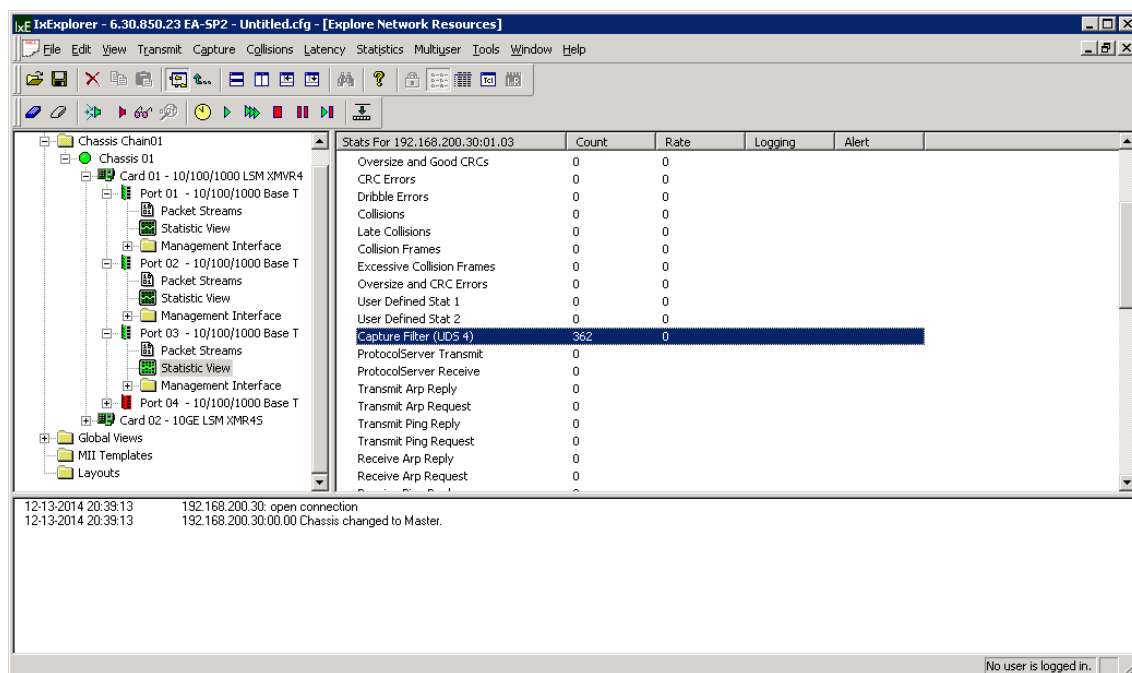
Program IxExplorer se hodí spíše pro specifické testy na určité rámce/pakety nebo určité požadavky na test/sít. Nejlepší je nakonfigurovat zařízení a konfiguraci uložit jako TCL skript a dále ho spustit pro zopakování stejného nastavení a testu.

Na obrázku 4.4 je ukázka nastavení toků na portu 1. Jsou kontinuálně posílané tři skupiny toků, první skupina má špatnou velikost rámce, druhá je správná a třetí má špatný CRC součet.

	Enable	Suspend	Name	Flow	Control	Loop Count	Frame Size	Data Pattern Type
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>			Continuous Packet	1	59	Inc Byte
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>			Continuous Packet	1	64	Inc Byte
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>			Continuous Packet	1	64	Inc Byte

Obr. 4.4: Nastavení skupin toku dat

Na 4.5 jsou zobrazeny statistiky zachytávání rámců na portu 3. Kromě typických údajů, jako celkový počet přijatých rámců a kolik rámců bylo odesláno/přijato, se dají zobrazit i údaje, které si uživatel sám nadefinuje, tzv. UDS filtr (User Defined Stat).



Obr. 4.5: Zobrazení statistik na portu 3

## 4.3 IxAutomate

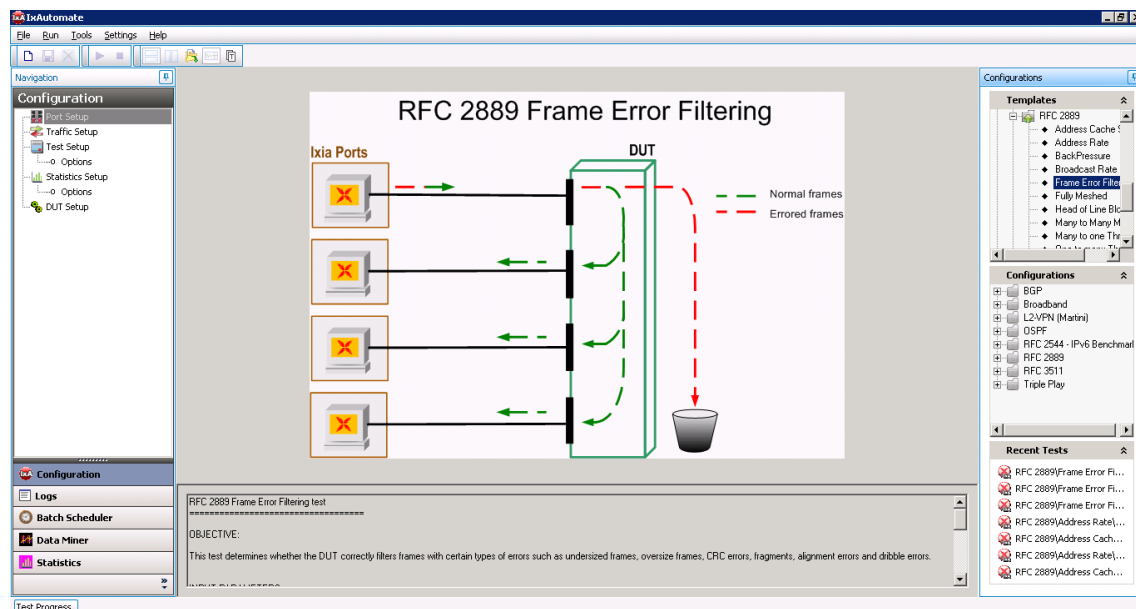
IxAutomate je GUI program napsán v C/C++ na testování síťových zařízení a sítí. Oproti IxExploreru už obsahuje standardizované testy z RFC, nazývají se „RFC Benchmark Software Bundle“. Pro testování přepínačů a směrovačů je určen balíček RFC 2544 - IPv6 Benchmark Test Suite. Může zjistit rychlost konvergence určitého protokolu, maximální počet cest pro každý protokol a dále klasické testy podle doporučení RFC 2544 (propustnost, ztrátovost...). Pro testování přepínačů je tu RFC 2889. Lze dokonce testovat i rychlost konvergence protokolů STP, MSTP a RSTP.

Nevýhodou je nutnost pro každý RFC test zakoupit licenci. Výhodou je rychlé předdefinované testování, kdy se nemusí detailně nastavovat každý parametr měření (např. toky dat...), jako v případě IxExploreru, ale dají se i zde použít TCL skripty (konfigurace se uloží jako TCL skript) [8].

### 4.3.1 Stručný popis IxAutomate

Stejně jako v případě IxExplorer, tak i tento program se spouští přes jiný počítač a vzdáleně se připojuje na generátor Ixia. Jako ukázka testování poslouží Error Frame Filtering test na přepínači Cisco z RFC 2889. Na obrázku 4.6 je okno programu po otevření. V obrázku nahoře je klasické menu s možností „File, Run, Tools,...“

Vlevo je menu pro konfiguraci určitého testu (*Configuration*) a zobrazení výsledků v podobě dat a grafů (*Data Miner* a *Statistics*). Testy se vybírají vpravo nahoře v menším menu (*Configuration - Templates*).



Obr. 4.6: Okno programu po spuštění

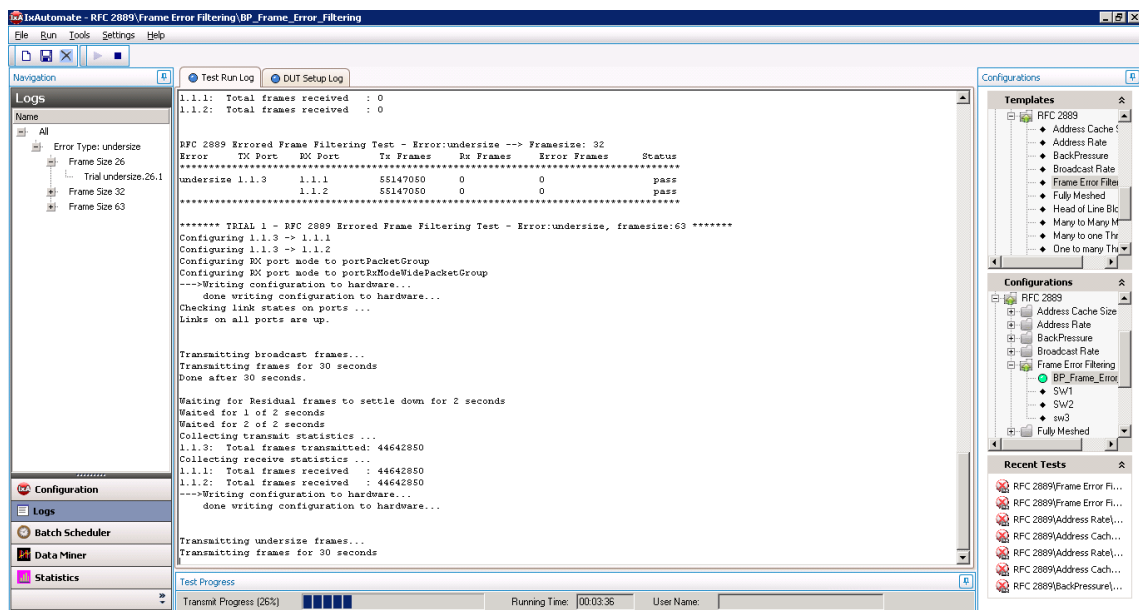
Pro ukázkou je vybrán RFC 2889 - Frame Error Filtering. Po kliknutí na příslušný test se uprostřed okna zobrazí stručný popis testu s jeho topologií. Podle doporučení se nový test vytváří následujícím postupem - pravým tlačítkem na příslušný test - *New Test* - libovolné jméno. Vytvořený test se zobrazí v menu vpravo (*Configuration*). V pravém dolním rohu je seznam nedávno použitých testů.

Test se spustí vlevo nahoře tlačítkem „*Start test*“. Průběh testu je na obrázku 4.7. V položce *Logs*, která je vlevo, je vidět posílané rámce - zkouší se chyba nedostatečné velikosti rámců. Dole na liště je čas (3:36), jak dlouho test běží a hned vedle nalevo je procentuální vyjádření průběhu zaslání (*Transmit Progress*).

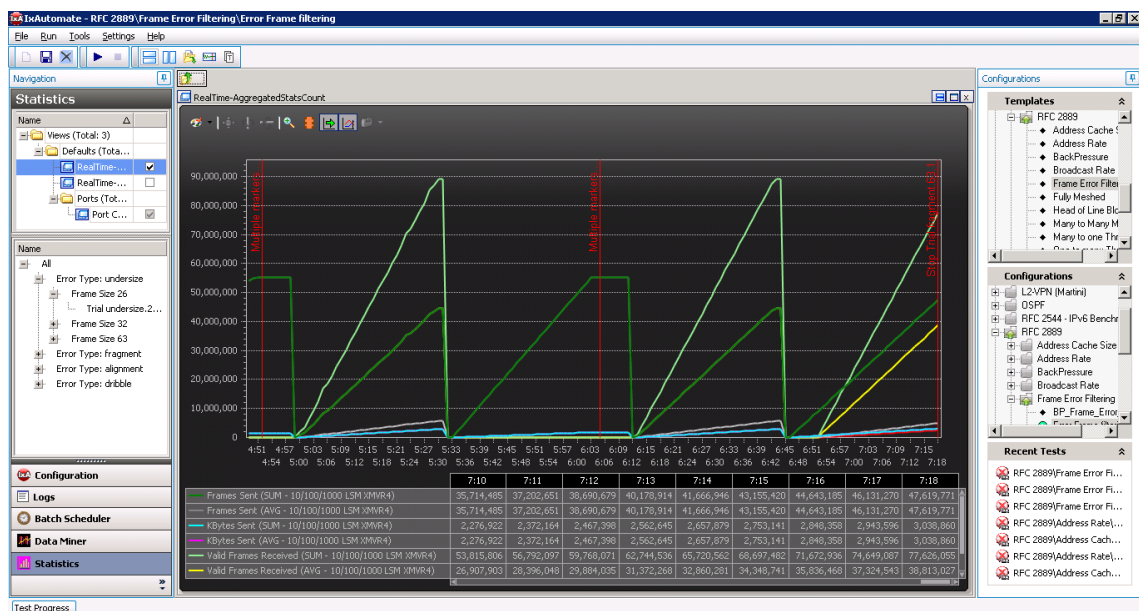
IxAutomate umí výsledky měření zpracovat do grafu. Po kliknutí na *Statistics* se zobrazí nahoře podokno s navigací mezi naměřenými udaji (*Navigation - Statistics*). Na 4.8 je ukáзка, jak takový graf vypadá.

## 4.4 ScriptGen

Užitečným programem je ScriptGen, který generuje TCL skripty aktuálního nastavení portů na Ixia generátoru. Měl by se používat po úspěšné konfiguraci v programu



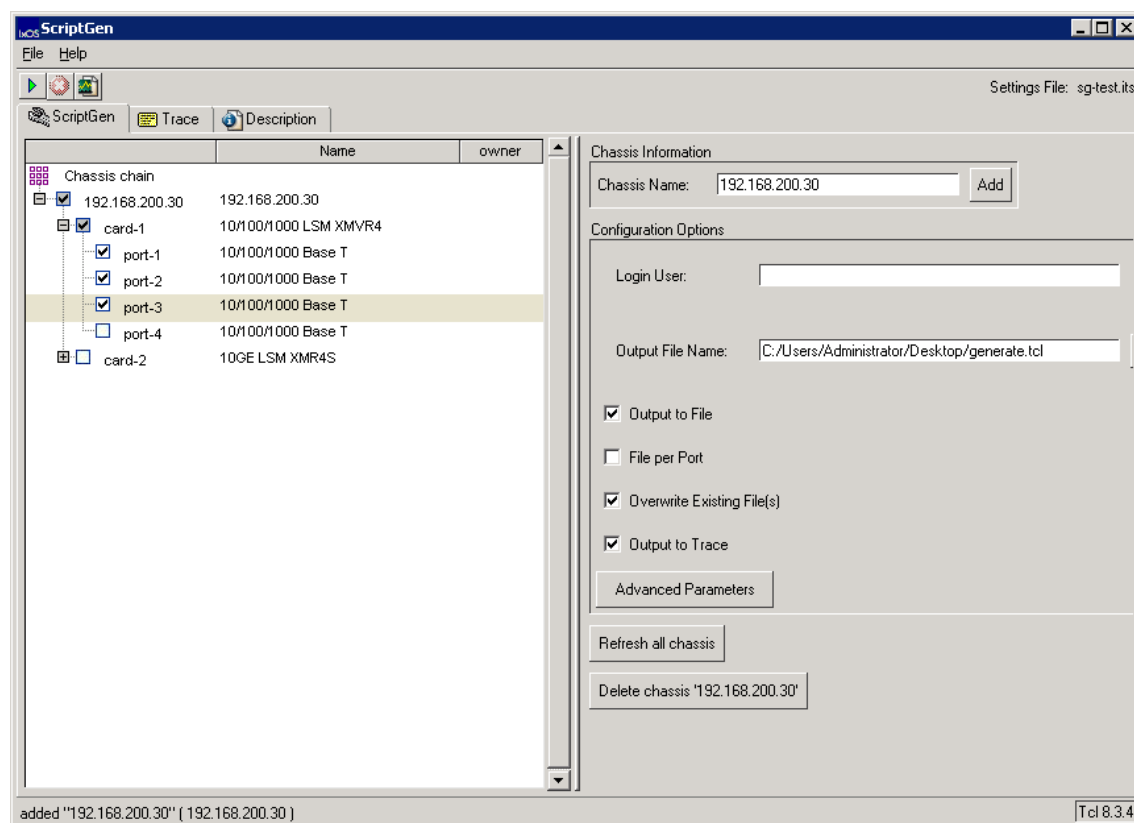
Obr. 4.7: Průběh testu Frame Error Filtering



Obr. 4.8: Grafické zobrazení statistiky měření

IxExplorer, IxAutomate nebo jiném obslužném programu. Hodí se pro znovu provedení stejného testu, kdy se zachová nastavení portů z předešlého testu. Běží jak na Linuxovém operačním systému, tak na systému Windows.

Na 4.9 je ukázka uložení aktuálního nastavení portů 1-3, karty 1, šasi s IP adresou 192.168.200.30. Je to nastavení po testu Error Frame Filtering. Lze zvolit možnost uložení nastavení do jednoho TCL souboru nebo pro každý port zvlášť (File per Port).



Obr. 4.9: Vytvoření TCL skriptu pomocí ScripGen programu

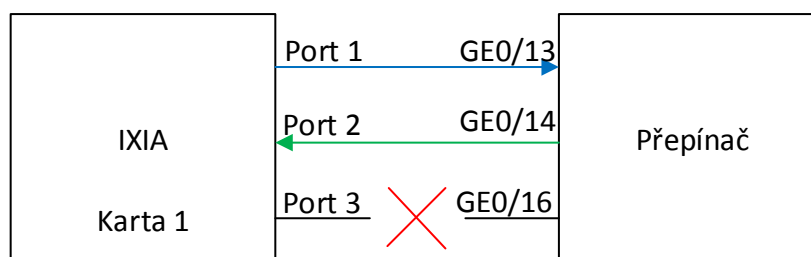
## 5 NÁVRH LABORATORNÍCH ÚLOH

### 5.1 Laboratorní úloha 1

První úloha by měla sloužit pro seznámení se s softwarovým prostředím testeru, konkrétně s programem IxAutomate. Studenti by si měli vyzkoušet ovládání a princip testování sítí na jednoduchém testu. Pro tuto úlohu stačí 2 porty DUT, které se propojí s IXIA generátorem. Jako DUT v tomto případě poslouží Cisco přepínač WS-C2960G-48TC-L (48 GigabitEthernet portů) s operačním systémem IOS verze 12.2 (35) SE5.

### Testování propustnosti a omezení provozu na přepínači

#### 5.1.1 Topologie měření



Obr. 5.1: Zapojení úlohy v laboratoři

Modrá barva zobrazuje generovaný provoz z generátoru, zelená vracející se ke generátoru. Provoz je z portu 1 (GE0/13) do portu 2 (GE0/14). Port 3 (GE0/16) není potřeba a je tak odpojen příkazem shutdown.

#### 5.1.2 Potřebná výbava

- 1 přepínač (CISCO 2960 s CISCO IOS verze 12.2 (35) SE5)
- IXIA generátor/analyzátor
- počítač s obslužným softwarem IXIA generátoru a přepínače (IxAutomate, PuTTY program pro připojení na přepínač)



### 5.1.3 Úvod

#### Propustnost (Throughput)

Propustnost se měří na linkové nebo na síťové vrstvě. Je to maximální možná rychlost, při níž nedochází ke ztrátám dat, v našem případě je to maximální počet rámců odesílaných z jednoho portu, na druhý bez jediné ztráty rámce. Je jednou ze základních parametru určující kvalitu služeb VoIP, video a audio přenosu, vedle zpoždění, ztrátovosti a jitteru, což jsou kritické parametry pro QoS (Quality of Service).

Při vysoké propustnosti dochází k rychlé konvergenci sítě po změnách a k rychlému přeposílání rámců, kdy může být provozováno více různých druhů služeb, např. několik streamů, audio/video přenosu. Nedochází ke ztrátám a zahazování. Naopak nízká propustnost je indikátorem špatného návrhu sítě nebo špatné konfigurace některého z prvků sítě.

Měření se provádí tak, že nejdříve se pošlou rámce na DUT (Device Under Test) s maximální přenosovou rychlostí. Dále se porovná počet odeslaných a přijatých rámců. Pokud nastane chyba nebo ztráta rámce, přenosová rychlost se sníží na polovinu a test se opakuje. Pokud chyba nebo ztráta rámce nenastane, přenosová rychlost se zvýší o polovinu rozdílu přenosové rychlosti posledního a předposledního měření [14].

#### Výpočet maximální propustnosti

Režie protokolu Ethernet je počítána v procentech podle vztahu 5.1:

$$\text{Režie protokolu} = \frac{\text{Délka rámce} - \text{Délka dat}}{\text{Délka rámce}} \quad (5.1)$$

V případě výpočtu samotné efektivity protokolu potom platí vztah 5.2:

$$\text{Efektivita protokolu} = \frac{\text{Délka dat}}{\text{Délka rámce}} \quad (5.2)$$

Efektivita při maximální délce pole dat 1500 B je potom dána vztahem uvedeným v rovnici 5.3:

$$\text{Maximální efektivita protokolu} = \frac{1500}{1538} \times 100 = 97.53\% \quad (5.3)$$

V případě tagovaných rámců (vlan tag), 1538 B včetně 12 B minimální mezery mezi rámci + 4 B vlan tag = 1538 B + 4 B vlan tag = 1542 B. Maximální efektivita je potom vyjádřena vztahem 5.4:

$$\text{Maximální efektivita protokolu} = \frac{1500}{1542} \times 100 = 97.28\% \quad (5.4)$$

Propustnost linky je počítána z celkové efektivity dle vztahu 5.5:

$$\text{Propustnost} = \text{Efektivita} \times \text{Přenosová rychlost} \quad (5.5)$$

Výpočet se řídí podle použitého média a jeho standardu, tj. 10 Mb/s, 100 Mb/s, 1 Gb/s, 10 Gb/s. a podle uvedeného vztahu 5.5 tedy bude pro 100 Mb/s linku platit vztah 5.6:

$$\begin{aligned} \text{Propustnost při 1500 B data} &= 0.9728 \times 100(Mb) = 97,28 Mb/s \\ \text{Propustnost při 64 B data} &= 0.0146 \times 100(Mb) = 1,46 Mb/s \end{aligned} \quad (5.6)$$

## Omezení provozu na přepínači

V některých případech je potřeba na přepínači snížit nebo omezit provoz, např. když klient u operátora zakoupil určitou šířku pásma, ale linka k němu má větší šířku pásma, než za jakou klient platí. Konkrétně může být maximální přenosová rychlost linky 1 Gbps nebo 10 Gbps, ale klient má zakoupenou rychlost 30 Mbps nebo 3 Gbps, také může být na druhé straně jiná maximální podporovaná rychlost. Právě v takových případech se hodí omezení provozu (rychlosti) na přepínači. Existuje několik způsobů jak toho dosáhnout [16]:

- Rychlost na portu (10, 100, 1000)
- `srr-queue`<sup>1</sup> příkazu
- Pomocí policeru (aggregate policer nebo obyčejná police-map)

V této úloze budou ukázány pro jednoduchost a z časových důvodů jen varianty omezení pomocí `srr-queue` a policeru. Případné zájemce odkazují na internet nebo jiné kurzy k tomu určené.

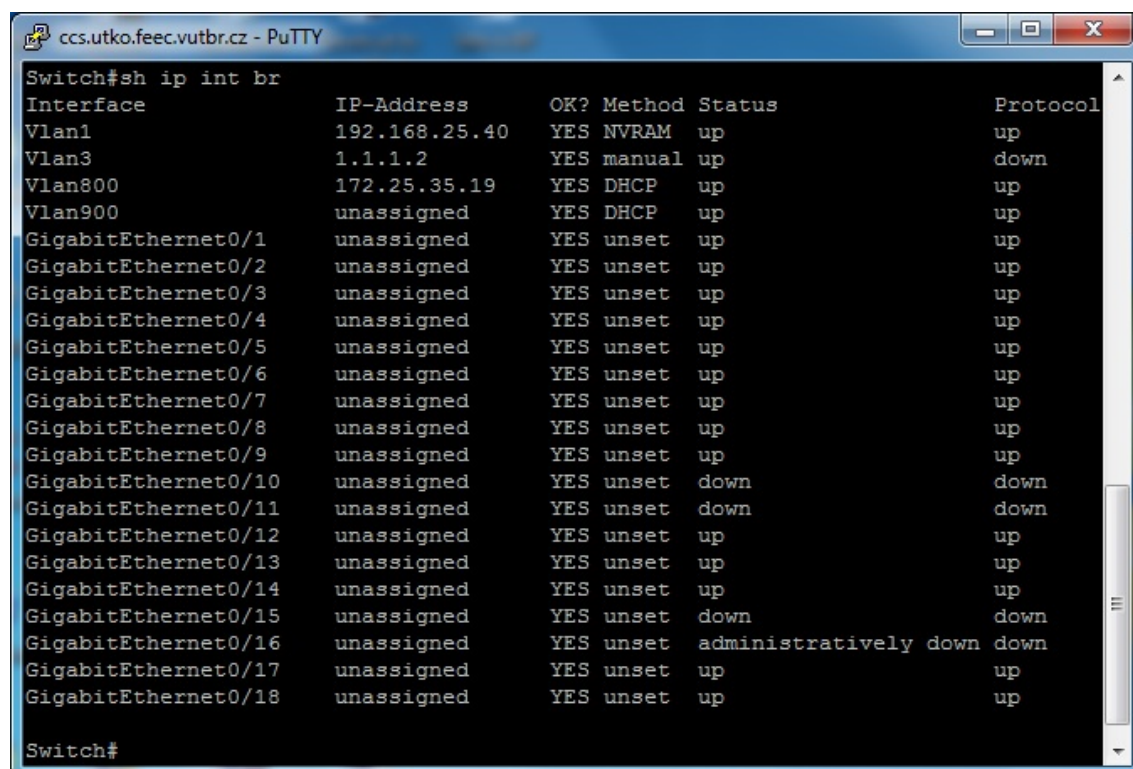
---

<sup>1</sup>SRR - *Shared/Shaped Round Robin*. Všechny novější přepínače mají pouze tento plánovač front. *Shared Mode* dovoluje využít šířku pásma jiné fronty, pokud je prázdná. *Shaped Mode* má přidělenou pevnou šířku pásma pro jednotlivou frontu. Více (v češtině) na WWW: <http://www.samuraj-cz.com/clanek/cisco-qos-5-qos-na-switchi-mls-srr-auto-qos/>

### 5.1.4 Příprava přepínače

Nejdříve je potřeba ověřit stav portů pomocí příkazu **show interface ip brief** a případně port GigabitEthernet 0/16 (pokud tak není) shodit pomocí příkazu **shut**  
**tdown**:

Switch#: **show ip interface brief**



Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.25.40	YES	NVRAM	up	up
Vlan3	1.1.1.2	YES	manual	up	down
Vlan800	172.25.35.19	YES	DHCP	up	up
Vlan900	unassigned	YES	DHCP	up	up
GigabitEthernet0/1	unassigned	YES	unset	up	up
GigabitEthernet0/2	unassigned	YES	unset	up	up
GigabitEthernet0/3	unassigned	YES	unset	up	up
GigabitEthernet0/4	unassigned	YES	unset	up	up
GigabitEthernet0/5	unassigned	YES	unset	up	up
GigabitEthernet0/6	unassigned	YES	unset	up	up
GigabitEthernet0/7	unassigned	YES	unset	up	up
GigabitEthernet0/8	unassigned	YES	unset	up	up
GigabitEthernet0/9	unassigned	YES	unset	up	up
GigabitEthernet0/10	unassigned	YES	unset	down	down
GigabitEthernet0/11	unassigned	YES	unset	down	down
GigabitEthernet0/12	unassigned	YES	unset	up	up
GigabitEthernet0/13	unassigned	YES	unset	up	up
GigabitEthernet0/14	unassigned	YES	unset	up	up
GigabitEthernet0/15	unassigned	YES	unset	down	down
GigabitEthernet0/16	unassigned	YES	unset	administratively down	down
GigabitEthernet0/17	unassigned	YES	unset	up	up
GigabitEthernet0/18	unassigned	YES	unset	up	up

Obr. 5.2: Výsledný výstup příkazu show ip interface brief

Pokud není rozhraní GigabitEthernet 0/16 down, tak je potřeba zadat následující příkazy:

```
Switch#: configure terminal  
Switch(config)#: interface g0/16  
Switch(config-if)#: shutdown  
Switch(config-if)#: end
```

Nyní nakonfigurujte omezení provozu na portu GigabitEthernet 0/14. Postup konfigurace je následující: Nejdříve je potřeba QoS zapnout pomocí **mls qos**<sup>2</sup> v globál-

<sup>2</sup>MLS (MultiLayerSwitch), mimo klasického přepínání umožňuje funkce na vyšších vrstvách než L2 - např. v našem případě **DiffServ QoS**.

ním režimu a nakonfigurovat **aggregate-policer** (agregovaný policer), kde se určí rychlostní limity na lince a zacházení s rámcí po překročení tohoto limitu a aplikujeme na dále uvedenou policy-map. Konkrétně je to 30Mbps (průměrný datový tok - 30Mbps - mělo by být násobkem 1024) a velikost shluku (burstu) - 1000000 (1Mbit). Pak je třeba nakonfigurovat **mac access-list** (ACL) pro povolené MAC adresy - takto se provoz povoluje nebo omezuje pro určité MAC adresy. U nás to bude kvůli jednoduchosti a použitelnosti u jakéhokoliv portu, na všechny MAC adresy. Dále se vytvoří mapa třídy - **class-map**, která přiřadí rámce do třídy podle určitých parametrů, v našem případě namapujeme výše vytvořený mac access-list na class-map. Předposledním krokem je aplikování zacházení (politiky) s rámcí, tj. vytvoření **policy-map**. Poslední částí konfigurace je aplikování mapy na rozhraní GE 0/14 a to ve směru **input**<sup>3</sup> - v tomto směru je to zejména zahazování, tvarování (na výstupu je to vyvažování).

```
Switch#: configure terminal
Switch(config)#: mls qos
Switch(config)#: mls qos aggregate-policer Speed30Mbps 31457280
1000000 exceed-action drop
Switch(config)#: mac access-list extended allmacaddresses
Switch(config-ext-nacl)#: permit any any
Switch(config-ext-nacl)#: exit
Switch(config)#: class-map match-all Link_30Mbps
Switch(config-cmap)#: match access-group name allmacaddresses
Switch(config-cmap)#: exit
Switch(config)#: policy-map Policy_30Mbps
Switch(config-pmap)#: class Link_30Mbps
Switch(config-pmap-c)#: police aggregate Speed30Mbps
Switch(config-pmap-c)#: end
Switch#: configure terminal
Switch(config)#: interface g0/14
Switch(config-if)#: service-policy input Policy_30Mbps
Switch(config-if)#: no shutdown
Switch(config-if)#: end
```

Zbývá nakonfigurovat výstupní směr rozhraní GigabitEthernet 0/14 pro další část úlohy, kdy se bude měřit propustnost v obráceném směru (z portu GE 0/14 na port GE 0/13). V tomto případě aplikujeme jen politiku 80% využití linky ve směru z

---

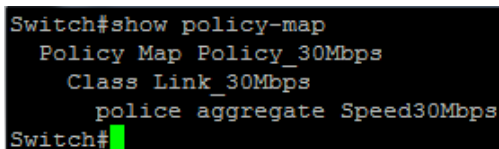
<sup>3</sup>Směr **output** se používá na VPN řešení v případě, kdy není možnost omezit datový tok přímo v přístupové síti.

portu, tzv. Engress pomocí příkazu **srr-queue bandwidth limit** *procento linky* (rozsah 10-90).

```
Switch#: configure terminal
Switch(config)#: interface g0/14
Switch(config-if)#: srr-queue bandwidth limit 80
Switch(config-if)#: no shutdown
Switch(config-if)#: end
```

Konfigurace přepínače je takto dokončená zbývá jen zkontrolovat správnost konfigurace. Výstupy příkazů by měly být shodné, jako na obrázcích dole. Pokud nejsou, tak je potřeba projít znovu konfiguraci. Je možné také použít příkaz **show run** na prohlédnutí všech nastavení najednou.

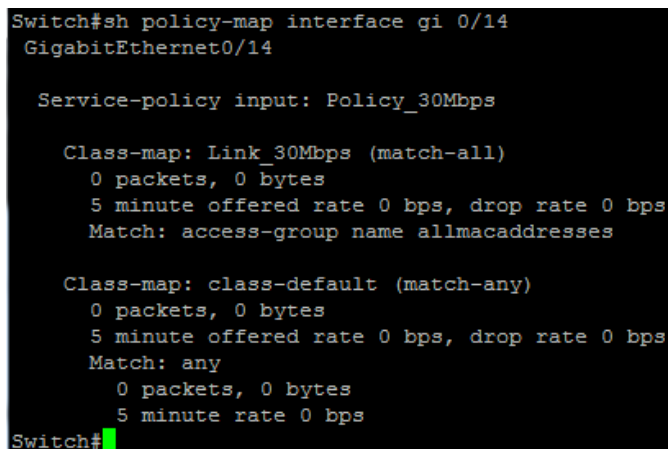
```
Switch#: show policy-map
```



```
Switch#show policy-map
  Policy Map Policy_30Mbps
    Class Link_30Mbps
      police aggregate Speed30Mbps
Switch#
```

Obr. 5.3: Výsledný výstup příkazu show policy-map pro ověření konfigurace politik

```
Switch#: show policy-map interface g0/14
```



```
Switch#sh policy-map interface gi 0/14
GigabitEthernet0/14

  Service-policy input: Policy_30Mbps

    Class-map: Link_30Mbps (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group name allmacaddresses

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
Switch#
```

Obr. 5.4: Výsledný výstup příkazu show policy-map interface g0/14 pro ověření aplikace politiky na rozhraní

Switch#: show run

```
no ip domain-lookup
!
mls qos aggregate-policer Speed30Mbps 31457000 1000000 exceed-action drop
mls qos
!
!
no errdisable detect cause gbic-invalid
no file verify auto
!
mac access-list extended allmacaddresses
 permit any any
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
class-map match-all Link_30Mbps
 match access-group name allmacaddresses
!
!
policy-map Policy_30Mbps
 class Link_30Mbps
  police aggregate Speed30Mbps
!
```

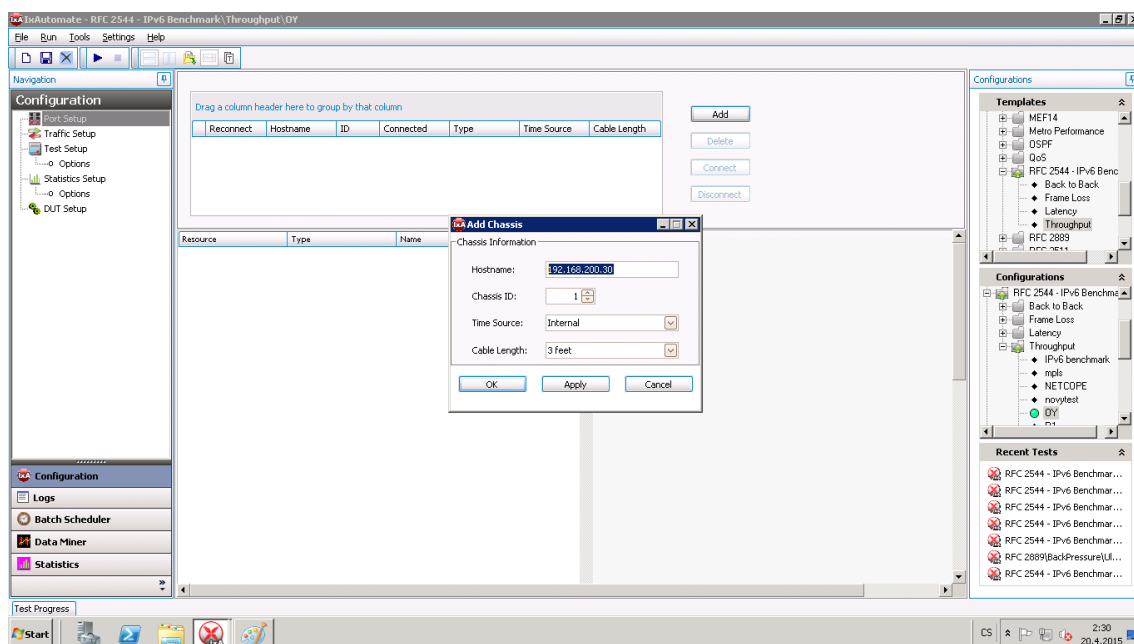
Obr. 5.5: Část výstupu příkazu show run

### 5.1.5 Nastavení IxAutomate a zahájení testu

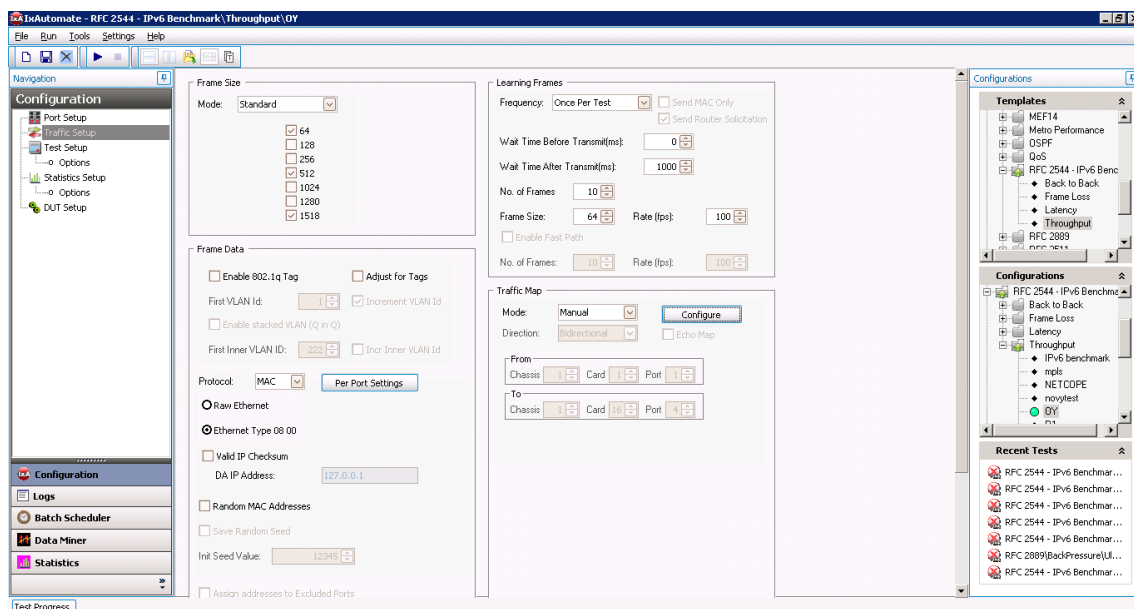
Pro spouštění testu propustnosti bude potřeba program IxAutomate, který je na ploše počítače. Po otevření programu z plochy, se otevře hlavní okno programu. Přejdeme do pravé části obrazovky, kde je záložka **Configuration Templates - RFC 2544 - Throughput** - pravým tlačítkem myši **New test** - zvolíme jakékoliv jméno, např. iniciály studentů na měření.

Otevře se obrazovka nastavení chassis generátoru - **Add** - všechno ponocháme a jen potvrdíme ok, viz 5.6. Přesuneme se do levé části obrazovky - levého menu - **Traffic Setup - Frame Size - Mode: Standard**, zvolíme velikost rámců 64, 512 a 1518 - viz 5.7. Velikosti rámců nám pro ukázkou stačí a v praxi se jedná u QoS o nejčastější možnost. Dále **Traffic Map - Mode: Manual - Configure** a vybereme směr provozu z karty 1, portu 1 (*Source Port*) na kartu 1, port 2 (*Destination Port*) - **Add - Apply**, viz 5.8. Zbytek necháme jak je.

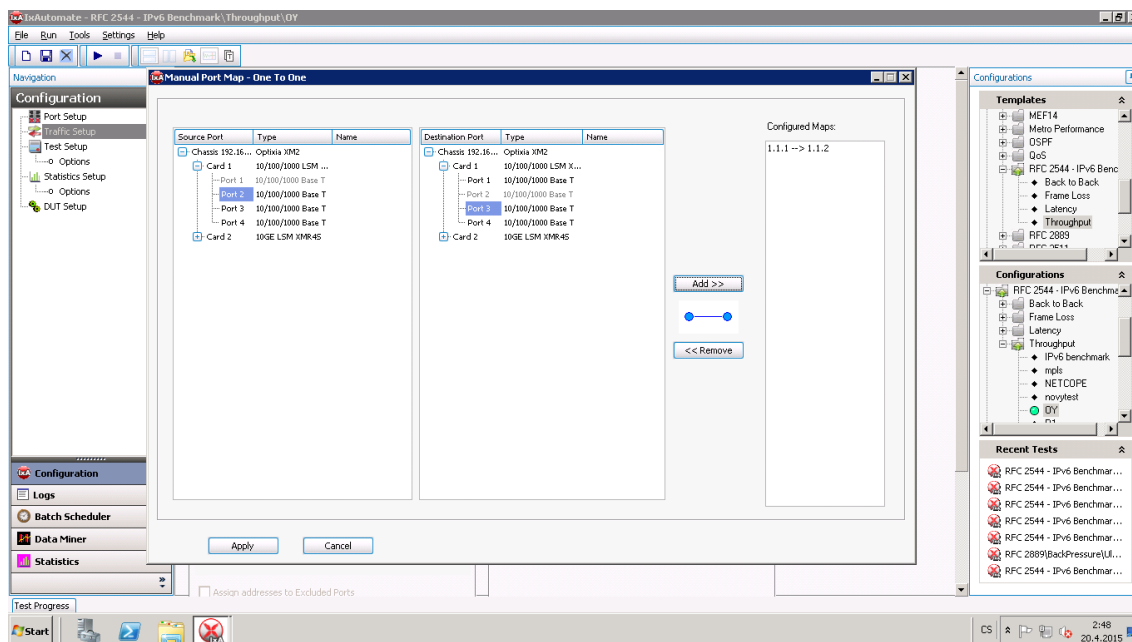
Nyní se přesuneme do **Test Setup - Duration** - pro naše testování stačí čas 10 sec. Teď už jen zbývá spustit testování trojúhelníkem (*Start*) vlevo nahoře, nebo klávesou F5. Test nějakou dobu trvá a může se kdykoliv zastavit čtvercem (*Stop*), nebo klávesou F6. Po čas testování se budou průběžně ukazovat výsledky v záložce **Logs** - jako na 5.9. Test skončí výpisem *Text Complete* a výsledky je možné grafický



Obr. 5.6: Nastavení chasis



Obr. 5.7: Nastavení parametrů testu



Obr. 5.8: Nastavení směru provozu

zobrazit ze záložky **Statistics**, viz 5.10. Pokud by záložka *Statistics* byla prázdná, tak stačí jen kliknout na malou ikonku složky v levém horním rohu (*Open*) - pak už jen stačí vybrat statistiku, kterou chceme sledovat.

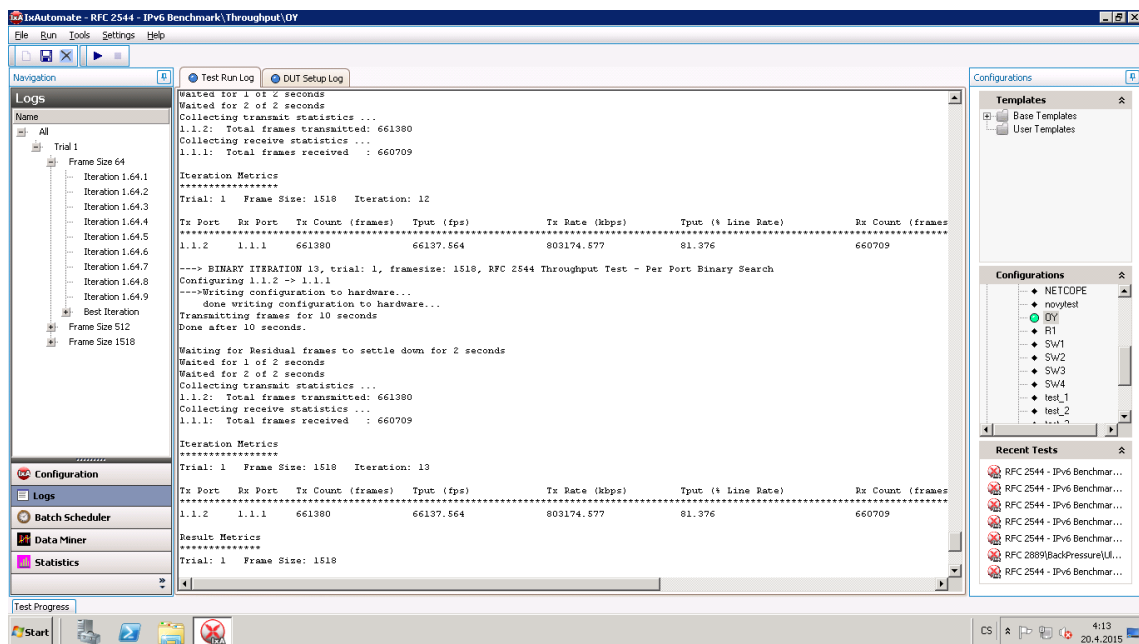
- Jaká je výsledná propustnost v daném směru?
- Proč je vždy na začátku testování, propustnost větší (i ztrátovost rámců), ale s počtem iterací se blíží námí nastavené?

Je vidět, že politika omezení provozu skutečně snížila propustnost na cca 30 Mbit/s, což je cca 3-4% využití linky v laboratoři. Velká propustnost na začátku měření je způsobená principem testování, kdy se při ztrátě rámce přenosová rychlost v daném směru snižuje o polovinu, dokud přenos tam a zpět neproběhne beze ztráty jediného rámce.

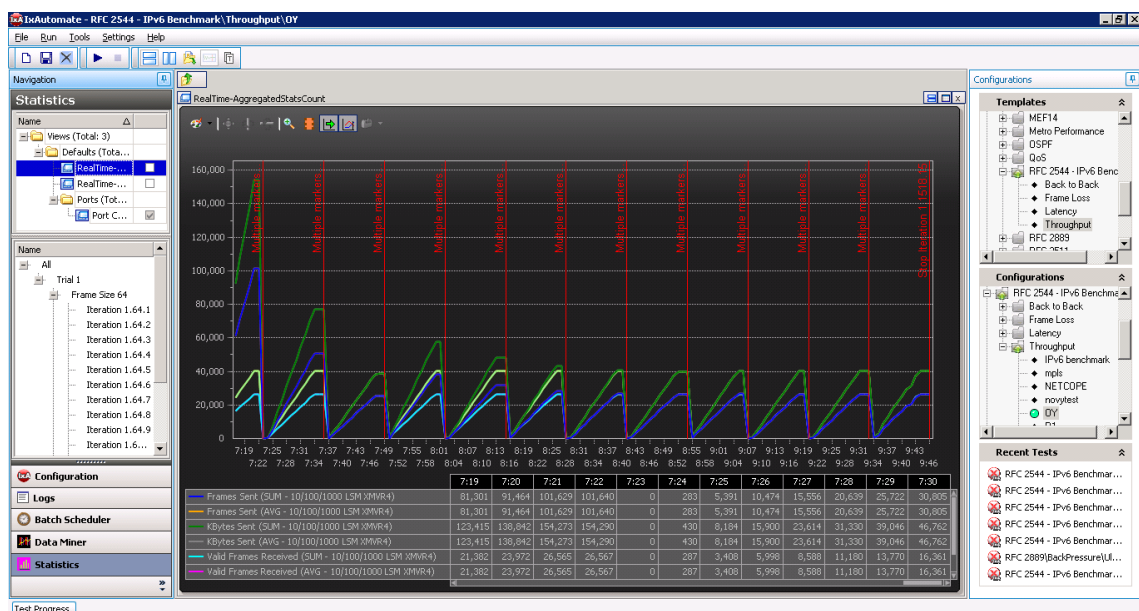
Otestujeme propustnost v obráceném směru - záložka vlevo **Configuration - Traffic Setup - Traffic Map** a známým způsobem (viz nahoře) nyní nastavíme provoz ve směru z karty 1, portu 2 na kartu 1, port 1 (předešlou mapu trafiky smažeme). Dále změním čas na 20 sec (kvůli správnosti testu při velikosti rámce 64) - **Test Setup - Duration** - 20 sec. Zpustíme nový test.

- Jaká je výsledná propustnost v tomto směru provozu a proč tomu tak je?





Obr. 5.9: Zaznamenávání průběhu testu v záložce *Logs*



Obr. 5.10: Ukázka grafického zobrazení výsledku testu

Propustnost v obráceném směru je větší, ale stále je tu omezení na 80% využití linky kvůli výše nastavenému příkazu srr-queue - výstupní směr rozhraní (obrázek 5.9). Propustnost je v rozmezí 78-82%, což odpovídá našemu předpokladu. Výsledné grafické zobrazení je na obrázku 5.11.



Obr. 5.11: Výsledné grafické zobrazení výsledků v opačném směru provozu

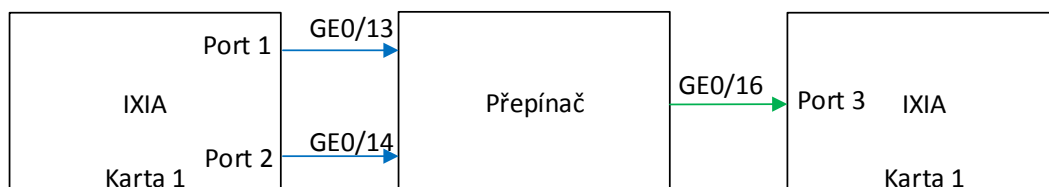
## 5.2 Laboratorní úloha 2

Druhá laboratorní úloha seznámí studenty s testováním kvality služeb - anglický QoS (Quality of Service) na linkové vrstvě (L2). Studenti by si měli vyzkoušet nastavit různé hodnoty CoS (Class of Service) pro jednotlivé toky rámců v programu IxExplorer a následně zahltit výstup jednoho portu na přepínači, kde budou vidět zahazování rámců s nižší prioritou CoS.

Pro tuto úlohu je potřeba tři portů na DUT zařízení. Jako DUT poslouží i v tomto případě Cisco přepínač WS-C2960G-48TC-L s operačním systémem IOS verze 12.2 (35) SE5.

# Testování kvality služeb na linkové vrstvě

## 5.2.1 Topologie měření



Obr. 5.12: Zapojení úlohy v laboratoři

Provoz je generován na dvou vstupních portech a směrován na jeden výstupní port, tj. z GE0/13 a GE0/14 na GE0/16, kde dojde k zahlcení. V programu IxExplorer jsou označené jako port 1, 2 a 3. Linky musí být v trunk<sup>4</sup> režimu (mode).

## 5.2.2 Potřebná vybava

- 1 přepínač (CISCO 2960 s CISCO IOS verze 12.2 (35) SE5)
- IXIA generátor/analyzátor
- počítač s obslužným softwarem IXIA generátoru a přepínače (IxExplorer, PuTTY program pro připojení na přepínač)

## 5.2.3 Úvod

### Kvalita služeb na linkové vrstvě

Moderní sítě mají tendenci více a více konvergovat video, audio a data přenosy do jednotné sítě. To znamená nárůst zátěže pro síť a s tím může docházet ke ztrátám a zpoždění rámců z důvodu např. jiného pořadí přijetí rámce než byl původně zaslán nebo zahlcení nějakého prvku v cestě. Společně s konvergencí roste i potřeba výrobců aktivních prvků (směrovačů a přepínačů) prokazovat schopnost podpory tzv. kvality služeb na jejích zařízeních. Podpora této funkce na linkové vrstvě urychluje přepínání rámců a redukuje čas zpracování rámců, protože není potřeba dívat se do hlavičky na síťové vrstvě. Mezi parametry, které se měří na linkové vrstvě, patří:

---

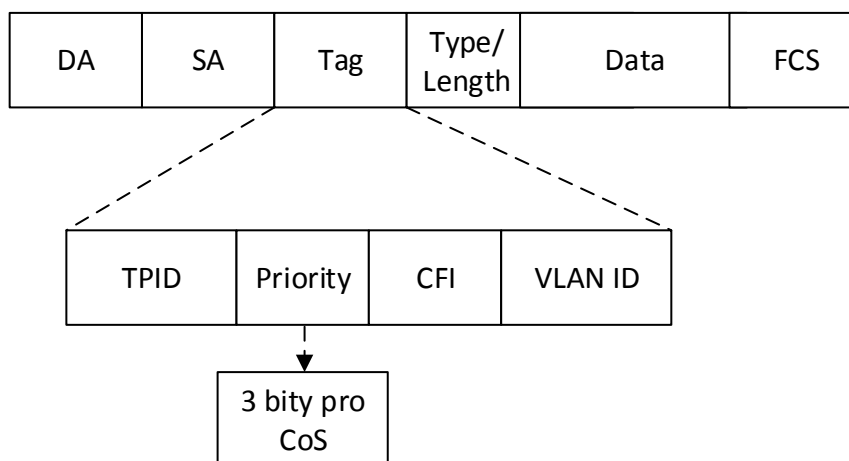
<sup>4</sup>Trunk režim značuje rámce, že patří do určité VLAN podle 802.1Q standardu - musí být nastaven na obou koncích linky.

- Throghput (Propustnost)
- Frame Loss (Ztrátovost rámců)
- Latency (Zpoždění)
- Jitter (kolísání zpoždění)

Tyto parametry se měří u různých tříd provozu, zatížení a velikosti rámců.

Kvalita služeb na linkové vrstvě (L2 QoS) může být dvojího typu. První je best-effort, což by se dalo nazvat „dělám co můžu“ - v tomto případě je zacházeno se všemi rámci stejně bez ohledu jestli jde o video, audio nebo data. Druhou možností je využít třídy služeb - Class of Service (dále jen CoS). CoS je definován standardem IEEE 802.1p a třídí jednotlivé provozy podle priority, kdy rámce s nižší prioritou jsou zahazovány přednostně [2] [15] [16] [3].

Pro třídění se využívají 3 bity v hlavičce značkováného Ethernet rámce standardu 802.1Q, tzv. tagged Ethernet frame<sup>5</sup> viz obrázek 5.13.



Obr. 5.13: Umístění CoS bitů v hlavičce rámce

Priorita může nabývat hodnot 0-7, kdy nejnižší je 0 a nejvyšší 7. Organizace IEEE doporučuje následující třídění, které je uvedené dále v tabulce 5.2.3.

<sup>5</sup>Rámeček, který je označen, že patří do určité VLAN, se nazývá značkováným rámcem (tagged frame).

Tab. 5.1: Doporučená klasifikace provozů podle IEEE

Uživatelská priorita	Typ provozu
1	Background (Data na pozadí)
2	Spare (Postradatelná data)
0	Best Effort
3	Excellent Effort
4	Controlled Load (Kontrolovaná zátěž)
5	„Video“ < 100 ms latency and jitter
6	„Voice“ < 10 ms latency and jitter
7	Network Control (Řídící data)

### 5.2.4 Příprava přepínače

Nejdříve je potřeba zkontrolovat jestli jsou rozhraní GE0/13, 0/14 a 0/16 up, pomocí příkazu **show ip interface brief** a popřípadě, když je nějaké down, tak zadat příkaz **no shutdown** a nastavit trunk režim na všech rozhraních pro VLAN 20. Zde je ukázka pro rozhraní GE0/13, ostatní se konfigurují analogicky.

```
Switch#: show ip interface brief
```

```
Switch#: configure terminal
```

```
Switch(config)#: interface g0/13
```

```
Switch(config-if)#: no shutdown
```

```
Switch(config-if)#: switchport mode trunk
```

```
Switch(config-if)#: switchport trunk allowed vlan 20
```

```
Switch(config-if)#: exit
```

```
Switch(config)#: int g0/14
```

```
Switch(config-if)#: ...
```

```
Switch(config-if)#: end
```

Dalším krokem je mapování CoS hodnot do vstupních a výstupních<sup>6</sup> front. Nastavení je následující: Příkazem **mls qos**<sup>7</sup> se aktivuje funkce QoS na přepínači a příkazem **mls qos srr-queue input cos-map queue <1-2>** (číslo vstupní fronty) **thre-**

<sup>6</sup>CISCO přepínač 2960 má dvě vstupní a čtyři výstupní fronty. Podrobnější popis dostupný na WWW: [http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2\\_50\\_se/configuration/guide/scg/swqos.html](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_50_se/configuration/guide/scg/swqos.html).

<sup>7</sup>MLS (MultiLayerSwitch), mimo klasického přepínání umožňuje funkce na vyšších vrstvách než L2 - např. v našem případě **DiffServ QoS**.

**shold** <1-3> (číslo prahu zahazování rámců) <0-7> (číslo CoS hodnot oddělené mezerou), přiřadit hodnoty CoS do jednotlivých front. Prahy zahazování 1-2 se nastavují (viz dále), práh 3 se nemění a zahazuje při 100% zaplnění fronty. Výstupní fronta se nastavuje podobně jako vstupní, jen místo **input** se použije **output**.

Vstupní fronty:

```
Switch#: configure terminal
Switch(config)#: mls qos
Switch(config)#: mls qos srr-queue input cos-map queue 1
threshold 2 1
Switch(config)#: mls qos srr-queue input cos-map queue 1
threshold 3 0
Switch(config)#: mls qos srr-queue input cos-map queue 2
threshold 1 2
Switch(config)#: mls qos srr-queue input cos-map queue 2
threshold 2 4 6 7
Switch(config)#: mls qos srr-queue input cos-map queue 2
threshold 3 3 5
```

Výstupní fronty:

```
Switch(config)#: mls qos srr-queue output cos-map queue 1
threshold 3 5
Switch(config)#: mls qos srr-queue output cos-map queue 2
threshold 3 3 6 7
Switch(config)#: mls qos srr-queue output cos-map queue 3
threshold 3 2 4
Switch(config)#: mls qos srr-queue output cos-map queue 4
threshold 2 1
Switch(config)#: mls qos srr-queue output cos-map queue 4
threshold 3 0
```

Dále je třeba nastavit jednotlivé prahy zahazování u jednotlivých vstupních a výstupních front. U vstupních front se tak děje pomocí příkazu **mls qos srr-queue input threshold** <1-2> (číslo vstupní fronty) <0-100> (velikost fronty 1 v procentech) <0-100> (velikost fronty 2 v procentech).

```
Switch(config)#: mls qos srr-queue input threshold 1 8 16
Switch(config)#: mls qos srr-queue input threshold 2 34 66
```

Prahy u výstupních front se nastavují trochu odlišně než u vstupních front. Na rozdíl od vstupu, musí se vytvořit set fronty, který se pak aplikuje na potřebné rozhraní a přidělení velikosti front může být v rozsahu 1-3200 procent. Příkaz vypadá takto: **mls qos queue-set output** <1-2> (číslo setu) **threshold** <1-4> (číslo fronty) <1-3200> (procento alokované paměti fronty pro zahazování) <1-3200> (procento alokované paměti fronty pro zahazování) <1-100> (garantované procento alokované paměti) <1-3200> (procento maxima paměti fronty).

```
Switch(config)#: mls qos queue-set output 2 threshold 1
149 149 100 149
Switch(config)#: mls qos queue-set output 2 threshold 2
118 118 100 235
Switch(config)#: mls qos queue-set output 2 threshold 3
41 68 100 272
Switch(config)#: mls qos queue-set output 2 threshold 4
42 72 100 242
```

Je možné přidělit i procento velikost bufferu pro vstupní a výstupní fronty. Konfigurace je následující:

```
Switch(config)#: mls qos queue-set output 2 buffers 16 6 17 61
Switch(config)#: mls qos srr-queue input buffers 67 33
```

Nakonec se může přidělit šířka pásma pro jednotlivé fronty na vstupu:

```
Switch(config)#: mls qos srr-queue input bandwidth 90 10
```

Zbývá aplikovat vytvořený set fronty na rozhraní GE0/16 - **queue-set 2**, aktivovat prioritní frontu na výstupu (fronta 1) - **priority-queue out** a přidáme ještě vyhrazené pásmo pro jednotlivé fronty - **srr-queue bandwidth share** <procento pro frontu 1> <procento fronta 2> <procento fronta 3> <procento fronta 4>.

```
Switch(config)#: int g0/16
Switch(config-if)#: queue-set 2
Switch(config-if)#: priority-queue out
Switch(config-if)#: srr-queue bandwidth share 10 10 60 20
Switch(config-if)#: end
```

Takto je konfigurace přepínače hotová. Můžeme se podívat na správnost jednotlivých nastavení pomocí následujících příkazů:

Switch#: show mls qos maps cos-input-q

```
Switch#show mls qos maps cos-input-q
Cos-inputq-threshold map:
      cos:  0    1    2    3    4    5    6    7
      -----
queue-threshold: 1-3 1-2 2-1 2-3 2-2 2-3 2-2 2-2
```

Obr. 5.14: Výstup příkazu show mls qos maps cos-input-q

Switch#: show mls qos maps cos-output-q

```
Switch#show mls qos maps cos-output-q
Cos-outputq-threshold map:
      cos:  0    1    2    3    4    5    6    7
      -----
queue-threshold: 4-3 4-2 3-3 2-3 3-3 1-3 2-3 2-3
```

Obr. 5.15: Výstup příkazu show mls qos maps cos-output-q

Switch#: show mls qos input-queue

```
Switch#show mls qos input-queue
Queue      :          1          2
-----
buffers    :          67          33
bandwidth  :          90          10
priority   :           0          10
threshold1 :           8          34
threshold2 :          16          66
```

Obr. 5.16: Výstup příkazu show mls qos input-queue



Switch#: show mls qos queue-set

```
Switch#show mls qos queue-set
```

Queueset: 1					
Queue	:	1	2	3	4
-----					
buffers	:	25	25	25	25
threshold1:		100	200	100	100
threshold2:		100	200	100	100
reserved	:	50	50	50	50
maximum	:	400	400	400	400

Queueset: 2					
Queue	:	1	2	3	4
-----					
buffers	:	16	6	17	61
threshold1:		149	118	41	42
threshold2:		149	118	68	72
reserved	:	100	100	100	100
maximum	:	149	235	272	242

Obr. 5.17: Výstup příkazu show mls qos queue-set (v úloze nastaven set 2)

### 5.2.5 Nastavení IxExplorer a zahájení testu

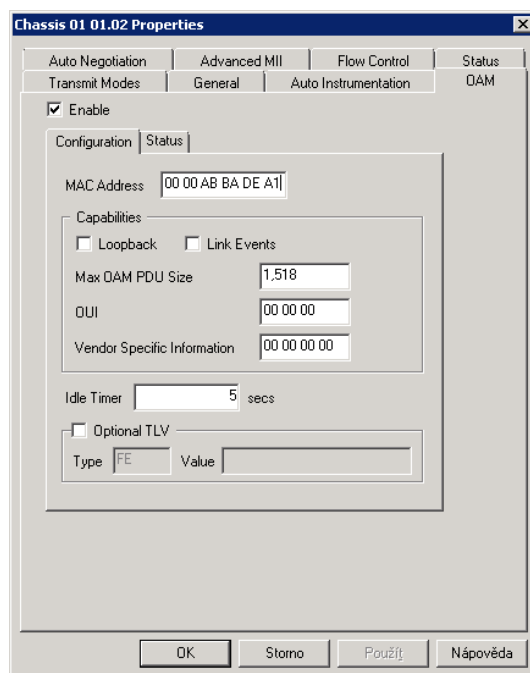
Na ploše PC klikněte na ikonu IxExplorer. Po otevření zadejte IP adresu šasi, která je 192.168.200.30 a potvrďte. V levém menu **Resources** (je tam chassis chain 01), rozklikněte **Card 01** a **porty 01-03**. Klikněte pravým tlačítkem na port 01 (potom analogický 02 a 03) a rozbalte záložku **OAM** - zatrhněte **Enable** (Zbytek nastavení necháme jak je) - původní MAC adresu můžete nechat (je ve tvaru 00 00 AB BA DE AD). U portu 02 a 03 změňte pouze koncový znak, jak je na obrázku 5.19. MAC adresy Ixia rozhraní si někam poznamenejte, budete je potřebovat dále.

Teď je potřeba nastavit jednotlivé streamy na portu 01, ale nejdříve si připravíme přehlednější tabulky a záložky streamu. **Port 01 - Packet Streams** - klikněte na 5.18 a přidejte do podokna **Visible Fields** - *Control*, *Frame Data*, *Vlan* a vše potvrďte.



Obr. 5.18: Tlačítko Add/Remove field from the table

Začněte vytvářet jednotlivé streamy. Pravým tlačítkem (v okně Packet Streams) - **New Stream** nebo **ALT + S** a nastavte podle 5.20.



Obr. 5.19: Ukázka aktivování MAC adresy Ixia na portu 02 se změnou posledního znaku

Přejděte to záložky (okno Packet Streams) **Gap/Rate Control - Desired % Line Rate** - 50, což ze dvou portů na výstupním 03 způsobí přetížení. Připravte si znamenované adresy z předchozího kroku. V záložce **DA/SA Data - DA Mode a SA Mode - Fixed**. Do *Destination Address* zadejte MAC adresu portu 03 a jako *Source Address*, adresu portu na kterém jsou dané streamy (nyní 01), viz 5.21.

	Name	Enable	Control	Flow	Loop Count	Suspend	Frame Size	Data Pattern Type	VLAN	VLAN ID	VLAN ID Count Mode	Repeat Count	VLAN User Priority	VLAN Canonical
1	Data	<input checked="" type="checkbox"/>	Advance	↓	1	<input type="checkbox"/>	512	Inc Byte	<input checked="" type="checkbox"/>	20	Idle	10	0	Reset
2	Video	<input checked="" type="checkbox"/>	Advance	↓	1	<input type="checkbox"/>	1,280	Inc Byte	<input checked="" type="checkbox"/>	20	Idle	10	4	Reset
3	Voice	<input checked="" type="checkbox"/>	Return to ID	↺	1	<input type="checkbox"/>	68	Inc Byte	<input checked="" type="checkbox"/>	20	Idle	10	5	Reset

Obr. 5.20: Nastavení streamů

	DA Mode	DA Value	DA Count	SA Mode	SA Value	SA Count
1	Fixed	00 00 AB BA DE A0	100	Fixed	00 00 AB BA DE AD	100
2	Fixed	00 00 AB BA DE A0	100	Fixed	00 00 AB BA DE AD	100
3	Fixed	00 00 AB BA DE A0	100	Fixed	00 00 AB BA DE AD	100

Obr. 5.21: Nastavení MAC adres

Klikněte na první stream *Data* - **Frame Data - Instrumentation** - zatrhněte **Time Stamp** a **Packet Group** - pod těmito parametry klikněte na tlačítko **Edit**

- dejte pozor, aby *Signature Offset* byl u všech streamů 48 a *Group ID Offset* 52 - **OK** - **OK**. Stejně nastavte ostatní streamy.

Nastavení toků na portu 02 probíhá obdobně jako na portu 01. Dejte pozor na offsety podpisování a skupiny (48 a 52) a rozdílnou zdrojovou MAC adresu.

Po dokončení konfigurace obou portů je potřeba nastavit filtrování paketů na portu 03 klikněte na něj - dále v horním menu **Capture - Filters** - záložka **Statistics** - **QoS** (toto můžete nastavit u zbylých dvou portech) - záložka **Receive Mode** - **Wide Packet Groups**, signature 48 a **PGID** 48 - dále záložka **Latency/Jitter** - **Latency/Jitter Measurement: Latency** a **Measurement Method: Store and Forward Latency** - **OK**.

V levém menu (kde je chassis, cart a porty) sjedte dolů a rozklikněte **Global Views** - **Statistic Views** - pravým tlačítkem **New** a vyberte tři porty (01, 02 a 03) - potvrďte. Takto budou vidět statistiky všech tří portů v jednom okně (včetně QoS rámců, pokud je nastaveno z předešlých kroků). Mezi okny se přepíná tak, že aktuální se minimalizuje a vybere jiné. Dále **Packet Group Statistic Views** - pravým tlačítkem **New** a vybereme port 03. V tomto vytvořeném okně se budou zaznamenávat výše zvolené zpoždění a latence.

Zbývá spustit samotný test. Děje se tak pomocí tlačítek 5.22. Ovládaní je velice intuitivní. Levá část označených tlačítek je pro start/stop zachytávání komunikace a pravá část pro start/stop samotných toků.



Obr. 5.22: Označená tlačítka na start/stop zachytávání a start/stop streamů

Před samotným spouštěním streamů se musí nejdříve označit port 03, kde bude zachycování rámců - tlačítko **Start Capture** a na portech 01, 02 **Start Transmit**. Teď otevřete statistiku *Packet Group Statistic Views* (v menu dole, kde jsou porty, karta a chassis) a obdobným tlačítkem jako *Start Capture* spusťte zaznamenávání dat pro statistiky. Výsledek by měl být podobný jako na 5.23. V případě potřeby můžete kliknout na *Card 01* - horní menu **Statistics - Clear All Statistics** - smaže statistiky na všech portech karty 01.

Je vidět, že nejmenší zpoždění je u PGID<sup>8</sup> 3, které odpovídá CoS 5 (PGID 1 - CoS 0, PGID 2 - CoS 4, PGID 3 - CoS 5).

Chassis: 192.168.200.30, Card: 01, Port: 03

PGID	Total # Frames Rec.	Latency Store Forward Min (μs)	Latency Store Forward	Latency Store Forward Max-Min (μs)	Latency Store Forward Avg (μs)	Bit Rate (/sec)	Byte Count
1	602,202	33,617,873.80	33,618,532.72	658.92	33,618,046.60	266,664,611	308,327,424
2	602,324	33,617,873.48	33,618,238.62	365.14	33,617,998.19	666,664,687	770,974,720
3	602,200	33,617,880.90	33,617,893.50	12.60	33,617,887.22	35,416,763	40,949,600

Obr. 5.23: Výsledné zpoždění a bitový tok

Dále je vidět i rozdílné přidělení pásma u jednotlivých priorit CoS - rozdílné bitové rychlosti PGID. PGID 2 (CoS 4) je video, ale jelikož máme nastavené sdílení pásem, tak se zahazují rámce i zde, aby se uvolnilo místo pro PGID 3 (CoS 5). Nejvíce se zahazují rámce u PGID 1 (CoS 0).

V případě zájmu a pokud zbyl čas, tak se můžete podívat na chování QoS při změnách rychlosti linek/toků, změnách CoS a případně přidat více streamů.

---

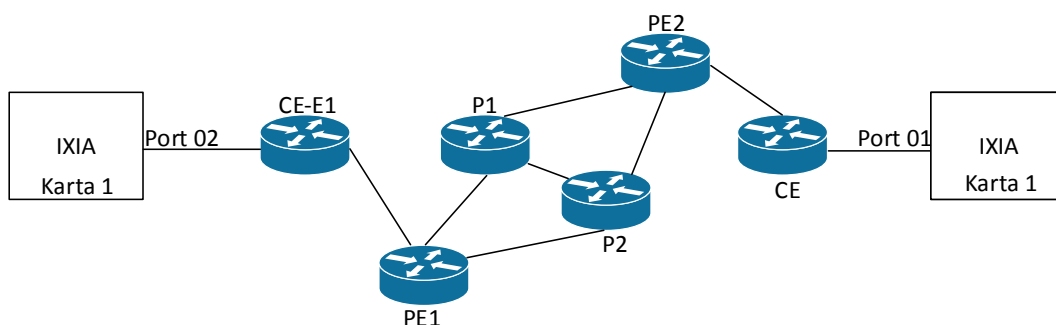
<sup>8</sup>PGID - *Packet Group Identifikation*, hodnoty které se nastavovaly u jednotlivých streamů. Automaticky se nastavuje tak, že PGID je stejné jako číslo streamu.

## 5.3 Laboratorní úloha 3

Třetí a poslední laboratorní úloha má za úkol změřit rychlost konvergence směrovacího protokolu OSPF, což je čas, kdy se ustálí všechny směrovací informace při změně topologie sítě, tj. např. výpadku linky, přidání dalšího uzlu (směrovače) apod. Výhodou této úlohy je, že navazuje na úlohu *směrování IP-MPLS* z předmětu VKS (vysokorychlostní síť).

## Testování rychlosti konvergence OSPF protokolu

### 5.3.1 Topologie měření



Obr. 5.24: Zapojení úlohy v laboratoři

Úloha navazuje na již vytvořenou topologii z úlohy předmětu VKS (vysokorychlostní síť) - *směrování IP-MPLS*. Port Ixia 02 je připojen na CE-E1, rozhraní směrovače FE0/0/3. Port Ixia 01 je připojen na CE, rozhraní směrovače FE0/0/3. Provoz bude generován z portu 02 na port 01 Ixia zařízení.

### 5.3.2 Potřebná výbava

- topologie a směrovače z úlohy *směrování IP-MPLS* z předmětu VKS
- IXIA generátor/analyzátor
- počítač s obslužným softwarem IXIA generátoru a směrovačů (ixExplorer, PuTTY program pro připojení na směrovače)

### 5.3.3 Úvod

#### Testování konvergence

Pojem konvergence souvisí s dynamickým směrováním. Je to stav při němž směrovač získá veškeré možné informace o topologii sítě, tzn. má informace od všech sousedů a zároveň sám poslal informace všem svým sousedům. Podmínkou je, aby tyto informace reflektovaly skutečný stav sítě. Zjednodušeně by se tento stav dal nazvat, kdy všichni mají informace o všech a na dané topologii sítě se shodnou. Je to významné měřítko výkonnosti směrovacích protokolů.

Směrovač se pokusí vyměnit informace o topologii sítě s ostatními směrovači. Rozsah této výměny, způsob jejího provedení a vyměňované informace závisí na použitém směrovacím protokolu (např. RIP, OSPF, BGP). Konvergovaný stav nastane poté, když jsou všechny informace rozeslány všem směrovačům, zapojeným do sítě. Pokud nastane v síti jakákoliv změna, která ovlivní směrovací tabulky (např. výpadek linky, změna topologie...), dojde dočasně k porušení konvergence, které trvá do doby, než je změna ohlášena všem směrovačům a znovu se všechny informace ustálí.

Čas potřebný, aby se informace znovu ustálily, se měří při rychlosti konvergence směrovacích protokolů. V moderních sítích se požaduje, aby byl co nejmenší. Některým protokolům konvergence trvá v řádech minut, jako např. RIP, jiným v řádech sekund až milisekund (v závislosti na počtu směrovačů a topologii), např. OSPF [1].

#### OSPF protokol

Je adaptivní hierarchický distribuovaný směrovací protokol, tzv. link-state, provádějící změny v směrovacích tabulkách na základě změny stavu v síti. Jedná se o nejpoužívanější protokol uvnitř autonomních systémů.

Směrovače, používající tento protokol, si v pravidelných krátkých intervalech zvláštními zprávami (Hello) kontrolují spojení se svými sousedními směrovači. Při zjištění jakékoliv změny, zasílá oznámení všem směrovačům v síti, ty si pak podle nové informace přepočítají nové cesty v síti a podle toho upraví směrovací tabulky. Výpočet nejkratších cest se provádí Dijkstrovým algoritmem.

Dalším vylepšením tohoto protokolu je rozdělení autonomního systému na několik oblastí (proto hierarchický), ve kterých si směrovače vzájemně vyměňují sdělení o změnách v síti, ale mimo svou oblast je neposílají. O výměnu souhrnných informací mezi oblastmi se starají hraniční směrovače. Touto technikou se zamezuje zahlcování rozlehlých sítí informacemi o změnách při velkém počtu směrovačů v autonomním systému [12].

### 5.3.4 Příprava směrovačů

Nejdříve je potřeba zjistit, jak jsou v topologii pakety směrované. Po připojení na směrovač CE-E1 stačí zadat příkaz **traceroute**. Projdeme cestu z CE-E1 na 172.17.60.1 (CE) - takto zjistíme přes který směrovač P (P1 nebo P2) vede cesta na CE.

CE-E1#: **traceroute 172.17.60.1**

```
CE-E1#traceroute 172.17.60.1

Type escape sequence to abort.
Tracing the route to 172.17.60.1

 1 172.17.1.1 0 msec 0 msec 0 msec
 2 172.16.1.1 [MPLS: Labels 16/24 Exp 0] 0 msec 0 msec 0 msec
 3 172.17.3.1 [MPLS: Label 24 Exp 0] 4 msec 0 msec 0 msec
 4 172.17.3.2 0 msec 0 msec *
CE-E1#
```

Obr. 5.25: Výstup příkazu traceroute na CE směrovač

Trasa vede přes směrovač P1 a pokud by se provedly následující příkazy na směrovačích, zjistilo by se, že konkrétně to je z FE0/0/0, PE1 na FE0/0/0, P1.

PE1#: **show ip interface brief**

```
PE1#show ip int br
Interface                               IP-Address      OK? Method Status      Prot
GigabitEthernet0/0                      192.168.25.52   YES NVRAM    up          up
GigabitEthernet0/1                      unassigned      YES NVRAM    administratively down down
FastEthernet0/0/0                       172.16.1.2      YES NVRAM    up          up
FastEthernet0/0/1                       172.16.4.2      YES NVRAM    up          up
GigabitEthernet0/1/0                    unassigned      YES NVRAM    administratively down down
FastEthernet0/2/0                       172.17.1.1      YES NVRAM    up          up
FastEthernet0/2/1                       unassigned      YES NVRAM    up          down
Loopback0                               10.1.1.3        YES NVRAM    up          up
```

Obr. 5.26: Výstup příkazu show ip int br na PE1

Rozhraní FE0/2/0 je vstupní do PE1 (je to první záznam z traceroute). Na PE1 se dále podíváme na druhý záznam z příkazu traceroute, pomocí **show ip route**.

PE1#: **show ip route**

```
C 192.168.25.0/24 is directly connected, GigabitEthernet0/0
  172.16.0.0/24 is subnetted, 5 subnets
C   172.16.4.0 is directly connected, FastEthernet0/0/1
O   172.16.5.0 [110/2] via 172.16.4.1, 5d02h, FastEthernet0/0/1
C   172.16.1.0 is directly connected, FastEthernet0/0/0
O   172.16.2.0 [110/2] via 172.16.1.1, 5d02h, FastEthernet0/0/0
O   172.16.3.0 [110/2] via 172.16.4.1, 5d02h, FastEthernet0/0/1
    [110/2] via 172.16.1.1, 5d02h, FastEthernet0/0/0
  10.0.0.0/32 is subnetted, 4 subnets
O   10.1.1.2 [110/2] via 172.16.4.1, 5d02h, FastEthernet0/0/1
C   10.1.1.3 is directly connected, Loopback0
O   10.1.1.1 [110/2] via 172.16.1.1, 5d02h, FastEthernet0/0/0
O   10.1.1.4 [110/3] via 172.16.4.1, 5d02h, FastEthernet0/0/1
    [110/3] via 172.16.1.1, 5d02h, FastEthernet0/0/0
```

Obr. 5.27: Výstup příkazu show ip route na PE1

Je vidět, že na adresy z rozsahu 172.16.1.0 vede rozhraní FE0/0/0 a pokud bychom se podívaly na P1 pomocí příkazu **show ip interface brief**, výstupem by bylo, že adresu 172.16.1.1 má rozhraní FE0/0/0 na P1, což je druhý záznam ve výše uvedeném traceroute.

P1#: **show ip interface brief**

```
P1#show ip int br
Interface                               IP-Address      OK? Method Status      Prot
ocol
GigabitEthernet0/0                     192.168.25.50   YES NVRAM    up          up
GigabitEthernet0/1                     unassigned      YES NVRAM    administratively down down
FastEthernet0/0/0                      172.16.1.1     YES NVRAM    up          up
FastEthernet0/0/1                      172.16.2.1     YES NVRAM    up          up
GigabitEthernet0/1/0                   unassigned      YES NVRAM    administratively down down
FastEthernet0/2/0                      172.16.3.1     YES NVRAM    up          up
FastEthernet0/2/1                      unassigned      YES NVRAM    administratively down down
Loopback0                              10.1.1.1       YES NVRAM    up          up
```

Obr. 5.28: Výstup příkazu show ip interface brief na P1



Podíváme se do směrovací tabulky na PE2 (vysvětlení proč, bude dále). Cesta na 172.16.1.0 (druhý záznam příkazu traceroute - 172.16.1.1) vede přes FE0/0/0, který později shodíme příkazem **shutdown**.

PE2#: **show ip route**

```
C 192.168.25.0/24 is directly connected, GigabitEthernet0/0
  172.16.0.0/24 is subnetted, 5 subnets
O   172.16.4.0 [110/2] via 172.16.5.1, 00:04:30, FastEthernet0/0/1
C   172.16.5.0 is directly connected, FastEthernet0/0/1
O   172.16.1.0 [110/2] via 172.16.2.1, 00:03:30, FastEthernet0/0/0
C   172.16.2.0 is directly connected, FastEthernet0/0/0
O   172.16.3.0 [110/2] via 172.16.5.1, 00:04:30, FastEthernet0/0/1
    [110/2] via 172.16.2.1, 00:03:30, FastEthernet0/0/0
  10.0.0.0/32 is subnetted, 4 subnets
O   10.1.1.2 [110/2] via 172.16.5.1, 00:04:31, FastEthernet0/0/1
O   10.1.1.3 [110/3] via 172.16.5.1, 00:04:31, FastEthernet0/0/1
    [110/3] via 172.16.2.1, 00:03:32, FastEthernet0/0/0
O   10.1.1.1 [110/2] via 172.16.2.1, 00:03:32, FastEthernet0/0/0
C   10.1.1.4 is directly connected, Loopback0
```



Obr. 5.29: Výstup příkazu show ip route PE2

Z výše uvedeného rozboru trasy vyplývá, že provoz z CE-E1 na CE jde přes PE1, P1, PE2 a nakonec skončí u CE, známe i přes která rozhraní.

### 5.3.5 Nastavení IxExplorer a zahájení testu

Na ploše PC klikněte na ikonu programu IxExplorer - zadejte IP 192.168.200.30 - potvrďte. Vlevo rozklikněte **Chassis 01 - Card 01 - Port 01, 02**. U portu 01 a 02 - **Packet Streams** - smažte stávající streamy - pravé tlačítko - delete (nebo označit stream a klávesa DEL). Na obou portech pravým tlačítkem - **Properties - OAM - Enable - OK**.

Vyberte kterýkoliv port (01 nebo 02) a v pravém okně otevřete **IxRouter**. Vlevo u stromové struktury označte **Protocol Management** a zaškrtněte **ARP** a **PING**, viz 5.30.

	Port Description	Port Owner	Link	Enable ARP	Enable PING for IPv4
1	192.168.200.30:01:01 - 10/10			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	192.168.200.30:01:02 - 10/10			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Obr. 5.30: Nastavení protocol managementu

Je třeba nastavit IP adresy Ixia portu a směrování mezi nimi - **Protocol Interfaces** a proveďte nastavení podle obrázku 5.31.

	Port Description	Port Link	Interface Description	Enable	IPv4 Address	IPv4 Mask Width	Gateway
1	192.168.200.30:01:01 - 10/10		1 - 01:01 - 172.17.60.2/24	<input checked="" type="checkbox"/>	172.17.60.2	24	172.17.60.1
2	192.168.200.30:01:02 - 10/10		1 - 01:02 - 172.17.50.2/24	<input checked="" type="checkbox"/>	172.17.50.2	24	172.17.50.1

Obr. 5.31: Nastavení IP adres IXIA portu a směrování mezi nimi

Dole klikněte na záložku **MAC - Enable** u obou portu (obr. 5.32). Otevřete záložku **IPv4** - zaškrtněte **Auto Arp**, viz 5.33. Ostatní ponechte beze změny a okno IxRouteru zavřete.

	Port Description	Port Link	Interface Description	Enable	MAC Address	EUI-64 Id	MTU
1	192.168.200.30:01:01 - 10/100/1000 Base T		1 - 01:01 - 172.17.60.2/24	<input checked="" type="checkbox"/>	00 00 3F 03 E9 1A	02 00 3F FF FE 03 E9 1A	1,500
2	192.168.200.30:01:02 - 10/100/1000 Base T		1 - 01:02 - 172.17.50.2/24	<input checked="" type="checkbox"/>	00 00 3F 03 E9 1B	02 00 3F FF FE 03 E9 1B	1,500

Obr. 5.32: Nastavení MAC adres

	Port Description	Port Link	Interface Description	IPv4 Address	IPv4 Mask Width	Gateway	Auto Arp
1	192.168.200.30:01:01 - 10/100/1000 Base T		1 - 01:01 - 172.17.60.2/24	172.17.60.2	24	172.17.60.1	<input checked="" type="checkbox"/>
2	192.168.200.30:01:02 - 10/100/1000 Base T		1 - 01:02 - 172.17.50.2/24	172.17.50.2	24	172.17.50.1	<input checked="" type="checkbox"/>

Obr. 5.33: Nastavení ARP protokolu

Zbývá nakonfigurovat stream - **Port 02 - Packet Streams** - okno napravo pravým tlačítkem - **New Stream**. V záložce **Frame/Stream Data** proveďte následující konfiguraci jako na 5.34.

	Name	Enable	Control	Flow	Loop Count	Suspend	Frame Size	Data Pattern Type
1	Test	<input checked="" type="checkbox"/>	Continuous Packet		1	<input type="checkbox"/>	256	Inc Byte

Obr. 5.34: Nastavení packet streamu

Dvakrát potukejte na stream (např. tam kde je jméno) a otevřete záložku **DA/SA** (vlevo, střed okna) - dole zaškrtněte **From Protocol Interfaces** a vyberte druhou možnost místo *Unknown* (případně hlášení jen potvrďte) - **OK**. Zbytek nastavení není třeba měnit.

Přejděte do záložky **Gap/Rate Control - Desired % Line Rate** nastavte na 97 a někde si poznamenejte údaj **Packets/Sec/Burst**<sup>9</sup>. Ještě musíte nastavit

<sup>9</sup>Může byt např. 43 936, 731 rámců/s

cílovou IP adresu. Záložka **Link/IP Data - Data Link Layer: Ethernet II - L3 Protocol: Ipv4 - L4 Protocol: UDP - IP Dest Address: 172.17.60.2 - IP Dest Mode: Fixed.**

Přejděte do levé části obrazovky - stromová struktura **Resources** - rozklikněte **Global Views - Statistic Views** - pravým **New** - vyberte port 02 a 01, potvrďte. Takto jsou vedle sebe zobrazené statistiky obou portů, jako na 5.35.

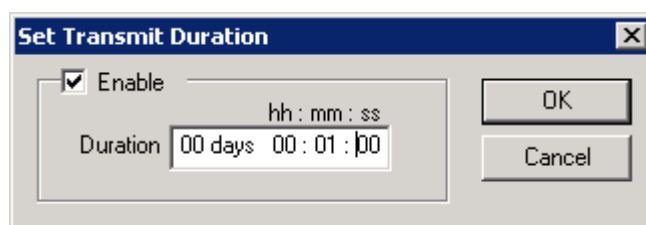
	A	B	C
1	Name	192.168.200.30:01.02	192.168.200.30:01.01
2	Link State	Link Up	Link Up
3	Line Speed	100 Mbps	100 Mbps
4	Duplex Mode	Full	Full
5	Frames Sent	0	0
6	Frames Sent Rate	0	0
7	Valid Frames Received	2	3
8	Valid Frames Received Rate	2	2
9	Bytes Sent	0	0
10	Bytes Sent Rate	0	0
11	Bytes Received	128	513
12	Bytes Received Rate	128	128
13	Fragments	0	0
14	Undersize	0	0

Obr. 5.35: Ukázka zobrazení statistik obou portů vedle sebe

Klikněte na 5.36, což nastaví čas přenosu paketů, nastavte podle 5.37.



Obr. 5.36: Ikona pro nastavení časování



Obr. 5.37: Nastavení doby přenosu

Připojte se na směrovač PE2. Zde budete shazovat rozhraní FE0/0/0 na P2. Pokud by se shodilo rozhraní FE0/0/0 u PE1, co vede na P1, tak by se konvergence nedala změřit (buď by byla ztrátovost paketů příliš malá nebo žádná), protože směrovač ví o obou cestách a rychlost přepojení na záložní cestu tak závisí na CPU (cca 20 ms).

V horním klasickém menu otevřete **Statistics - Clear All Statistics** a 5.38 spustíte stream (tlačítkem 5.39 se zastaví).



Obr. 5.38: Ikona na start streamu



Obr. 5.39: Ikona na zastavení streamu

Na směrovači PE2 zadejte následující příkazy na shození rozhraní FE0/0/0:

```
PE2#: conf t
PE2(config)#: int fa0/0/0
PE2(config-if)#: shutdown
```

Po zchození rozhraní dojde ke změně cesty na CE, což se projeví ztrátou rámců u streamu. Měli byste získat podobné výsledky jako na 5.40. Pokud jste výše uvedené nestihli do 1 min, tak změňte čas generování streamu nebo zkuste znovu (nezapomeňte promazat statistiky).

Name	192.168.200.30:01.02	192.168.200.30:01.01
Link State	Link Up	Link Up
Line Speed	100 Mbps	100 Mbps
Duplex Mode	Full	Full
Frames Sent	2,641,864	0
Frames Sent Rate	0	0
Valid Frames Received	54	2,399,312
Valid Frames Received Rate	0	0

Obr. 5.40: Předpokládané výsledky ztrátovosti paketů

Výsledný čas se vypočítá jako rozdíl přijatých a odeslaných paketů, podělený počtem generovaných paketů za sekundu, což je údaj, který jste měli zaznamenat dříve. Konvergence by měla mít cca 5,5 sec.

Po skončení měření nahodte zase zpět rozhraní FE0/0/0 na PE2:

```
PE2(config-if)#: no shutdown
```

```
PE2(config-if)#: end
```

## 6 ZÁVĚR

Bakalářská práce se věnuje problematice testování a následné analýze vysokorychlostních sítí, což jsou sítě s rychlostí větší než 100 Mbit/s. Dnes poměrně běžné 1 Gbit/s, 10 Gbit/s (na páteřních linkách) a více. V první kapitole je popsána technologie Ethernet, gigabitový Ethernet. Jsou tu rozebrány vrstvy z kterých se tyto technologie skládají a jejich popis. Celkově kapitola slouží pro uvedení do problematiky a její lepší pochopení - čtenář získá povědomí o technologii na které to vše tzv. „běží“.

Další kapitola obecně popisuje přepínač a směrovač, protože to jsou běžné prvky s jejichž podobou se můžeme setkat kdekoliv, ať už softwarovou nebo hardwarovou. Je stručně ukázána jejich funkce, zařazení do hierarchického uspořádání (v případě přepínače) a jak pracují, včetně jejich kladů a záporů.

Kapitola možnosti testování sítí se už věnuje čisté problematice sítí. Jsou tu uvedena nejpoužívanější v dnešních sítích referenční měření a použita v mé bakalářské práci - RFC 2544 pro všeobecné testování sítí, tj. testuje jak přepínače, tak směrovače. Následuje kapitola o síťovém analyzátoru IXIA a jeho balíčku obslužných programů - Ixexplorer, IxAutomate a ScriptGen. Stručně jsou popsány konfigurační možnosti.

Dále je praktická část s návrhem úloh. Dvě úlohy jsou zaměřené na linkovou vrstvu s různou konfigurací přepínače od celosvětové firmy Cisco. První úloha se zabývá měřením propustnosti při různé konfiguraci provozu na přepínači. Druhá úloha je zaměřená na kvalitu služeb linkové vrstvy, kde se na přepínači konfiguruje fronty, buffery, pásma a přiřazují se CoS (Class of Service) hodnoty jednotlivým frontám. Následně po konfiguraci v programu IxExplorer, se sleduje chování při různé zátěži výstupního portu přepínače. Třetí úloha se zabývá síťovou vrstvou a měří rychlost konvergence dynamického, tzv. link-state, směrovacího protokolu OSPF.

Jako doplněk je ke každé úloze vytvořena prezentace a konečná konfigurace programu IxAutomate a IxExplorer, např. pro případ, kdyby se studentům měla ukázat správná konfigurace.

# LITERATURA

- [1] Black Books. *Network Convergence Testing*. Edidion 10. Calabassas: Ixia, 2013, 51 s.
- [2] Black Books. *Quality of Service Validation*. Edition 10. Calabassas: Ixia, 2011, 73 s.
- [3] Cisco Switch Catalyst 2960 Configuration Guide. *Configuring QoS* [online] [cit. 24. 4. 2015]. Dostupné z URL: <<http://1url.cz/v01Z>>.
- [4] Cisco DocWiki. *Ethernet Technologies*. [online] 2009, poslední aktualizace 29.8.2014 Dostupné z URL: <[http://docwiki.cisco.com/wiki/Ethernet\\_Technologies](http://docwiki.cisco.com/wiki/Ethernet_Technologies)>.
- [5] Industrial ethernet book. *Addressing the needs and concerns for next generation 10Gb Ethernet*. [online]. © 2010-2014, poslední aktualizace 24. 11. 2014 [cit. 25. 11. 2014]. Dostupné z URL: <<http://www.iebmedia.com/index.php?id=5488&parentid=63&themeid=255&showdetail=true>>.
- [6] Ixia. *IxOS Getting Started Guide*. Release 6.30. Calabassas: Ixia, 2012, 90 s.
- [7] Ixia. *ExExplorer User Guide*. Release 6.30. Calabassas: Ixia, 2012, 1466 s.
- [8] Ixia. *IxAutomate User Guide*. Release 7.30. Calabassas: Ixia, 2012, 944 s.
- [9] LAMME, Todd. *CCNA: výukový průvodce přípravou na zkoušku*. 640-802. Vyd. 1. Brno: Computer Press, 2010, 928 s. ISBN 978-802-5123-591.
- [10] NOVOTNÝ, V. *Architektura sítí*. Vyd. 1. Brno: Vysoké učení technické v Brně Fakulta elektrotechniky a komunikačních technologií Ústav telekomunikací, 2012, 152 s. ISBN 978-80-214-4450-8.
- [11] Optical Systems Design. *Testing the capabilities of your ethernet network part I*. [online]. [cit. 7. 12. 2014]. Dostupné z URL: <<http://osd.com.au/testing-the-capabilities-of-your-ethernet-network-part-i/>>.
- [12] Open Shortest Path First. *Open Shortest Path First* [online]. Dostupné z URL: <[http://cs.wikipedia.org/wiki/Open\\_Shortest\\_Path\\_First](http://cs.wikipedia.org/wiki/Open_Shortest_Path_First)>.
- [13] Optical Systems Design. *Testing the capabilities of your ethernet network part II*. [online]. [cit. 7. 12. 2014]. Dostupné z URL: <<http://osd.com.au/testing-the-capabilities-of-your-ethernet-network-part-ii/>>.

- [14] RFC 2544. *Benchmarking Methodology for Network Interconnect Devices*. [IETF] 1999, Dostupné z URL: <<https://www.ietf.org/rfc/rfc2544.txt>>.
- [15] [www.samuraj-cz.com](http://www.samuraj-cz.com) *Cisco QoS 5 - praktické příklady použití QoS* [online] [cit. 24. 4. 2015]. Dostupné z URL: <<http://www.samuraj-cz.com/clanek/cisco-qos-5-qos-na-switchi-mls-srr-auto-qos/>>.
- [16] [www.samuraj-cz.com](http://www.samuraj-cz.com) *Cisco QoS 6 - praktické příklady použití QoS* [online] [cit. 24. 4. 2015]. Dostupné z URL: <<http://www.samuraj-cz.com/clanek/cisco-qos-6-prakticke-priklady-pouziti-qosu/>>.
- [17] ŠKORPIL, V. *Přístupové a transportní sítě*. Vyd. 1. Brno: Vysoké učení technické v Brně Fakulta elektrotechniky a komunikačních technologií Ústav telekomunikací, 2012, 128 s. ISBN 978-80-214-4457-7.



# SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

ACL Access Control List

API Application Programming Interface

BMWG Benchmarking Methodology Working Group

CAM Content Addressable Memory

CFI Canonical Format Indicator

CSMA/CD Carrier Sense Multiple Access with Collision Detection

CoS Class of Service

DUT Device Under Test

FCS Frame Check Sequence

FIB Forwarding Information Base

FPS Frames per Second

GbE Gigabit Ethernet

HSSG Higher Speed Study Group

ID Identification

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IFG Interframe gap

IOS Internetwork Operating System

IP Internet Protocol

IPv4 Internet Protocol version 4

IPv6 Internet Protocol version 6

ISO International Standards Organization

ITU International Telecommunication Union

LAN Local Area Network

LLC Logical link control

MAC Media Access Control

MLS Multilayer Switching

OSI Open Systems Interconnection

PC Personal Computer

PCS Physical Coding Sub-layer

PHY Physical layer

PMA Physical Medium Attachment Sublayer

PMD Physical Medium Attachment

QoS Quality of Service

RFC Request for Comments

VLAN Virtual Local Area Network

VoIP Voice Over Internet Protocol

WAN Wide Area Network

# SEZNAM PŘÍLOH

A Obsah přiloženého CD

67

## A OBSAH PŘILOŽENÉHO CD

- Soubor BP\_prace (Bakalářská práce ve formátu „.PDF“)
- Složka souborů „Koncova\_konfigurace“ (Koncová konfigurace úloh v podobě TCL skriptů)
- Složka souborů „Prezentace\_k\_uloham“ (Prezentace k jednotlivým laboratorním úlohám ve formátu „.PPT“)